

Method and apparatus for security in a data processing system

Publication number: JP2004532554 (T)

Publication date: 2004-10-21

Inventor(s):

Applicant(s):

Classification:

- international:

G06F21/00; H04B7/26; H04L12/18; H04L12/56; H04L29/06; H04L29/08; H04L9/08; H04L9/16; H04W12/02; H04W28/06; H04W28/18; H04W72/04; H04W80/00; H04W92/10; H04L9/30; H04W28/04; H04W4/00; H04W52/02; G06F21/00; H04B7/26; H04L12/18; H04L12/56; H04L29/06; H04L29/08; H04L9/08; H04L9/14; H04W12/00; H04W28/02; H04W28/16; H04W72/00; H04W80/00; H04W92/00; H04L9/28; H04W4/00; H04W52/00; (IPC1-7): H04B7/26; H04L9/16; H04Q7/38

- European:

G06F21/00N9T; H04L12/18; H04L12/56B; H04L29/06; H04L29/06C2; H04L29/06C5; H04L29/06M4S2; H04L29/06M6E; H04L29/06M6P; H04L29/06N; H04L29/06S16C; H04L29/06S4B; H04L29/06S6A; H04L29/06S6E; H04L29/08N13; H04L29/08N21; H04L29/08N3; H04L9/08B; H04Q7/38W; H04W12/04

Application number: JP20020577334T 20020328

Priority number(s): US20010279970P 20010328; US20010933972 20010820; WO2002US09835 20020328

Also published as:

JP4282992 (B2)
US2002141591 (A1)
WO02080449 (A1)
TW550926 (B)
MXPA03008923 (A)

more >>

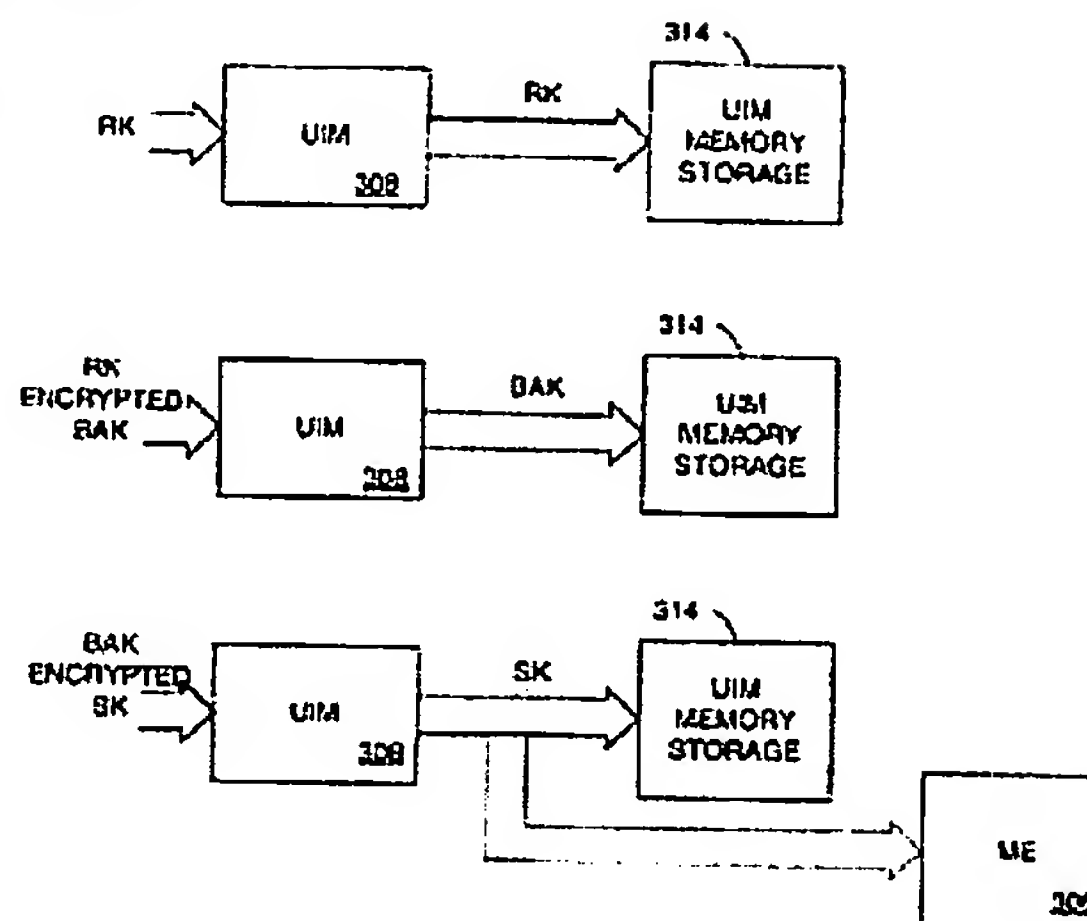
Abstract not available for JP 2004532554 (T)

Abstract of corresponding document: US 2002141591 (A1)

Method and apparatus for secure transmissions.

Each user is provided a registration key. A long-time updated broadcast key is encrypted using the registration key and provided periodically to a user.

A short-time updated key is encrypted using the broadcast key and provided periodically to a user. Broadcasts are then encrypted using the short-time key, wherein the user decrypts the broadcast message using the short-time key.



Data supplied from the *espacenet* database — Worldwide

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2004-532554

(P2004-532554A)

(43) 公表日 平成16年10月21日(2004.10.21)

(51) Int.Cl. ⁷	F I	テーマコード (参考)
H04B 7/26	H04B 7/26 M	5J104
H04L 9/16	H04L 9/00 643	5K067
H04Q 7/38	H04B 7/26 109R	

審査請求 未請求 予備審査請求 有 (全 76 頁)

(21) 出願番号	特願2002-577334 (P2002-577334)	(71) 出願人	595020643
(86) (22) 出願日	平成14年3月28日 (2002.3.28)		クualコム・インコーポレイテッド
(85) 翻訳文提出日	平成15年9月29日 (2003.9.29)		QUALCOMM INCORPORATED
(86) 国際出願番号	PCT/US2002/009835		アメリカ合衆国、カリフォルニア州 92
(87) 国際公開番号	W02002/080449		121-1714、サン・ディエゴ、モア
(87) 国際公開日	平成14年10月10日 (2002.10.10)		ハウス・ドライブ 5775
(31) 優先権主張番号	60/279,970	(74) 代理人	100058479
(32) 優先日	平成13年3月28日 (2001.3.28)		弁理士 鈴江 武彦
(33) 優先権主張国	米国 (US)	(74) 代理人	100091351
(31) 優先権主張番号	09/933,972		弁理士 河野 哲
(32) 優先日	平成13年8月20日 (2001.8.20)	(74) 代理人	100088683
(33) 優先権主張国	米国 (US)		弁理士 中村 誠
		(74) 代理人	100109830
			弁理士 福原 淑弘

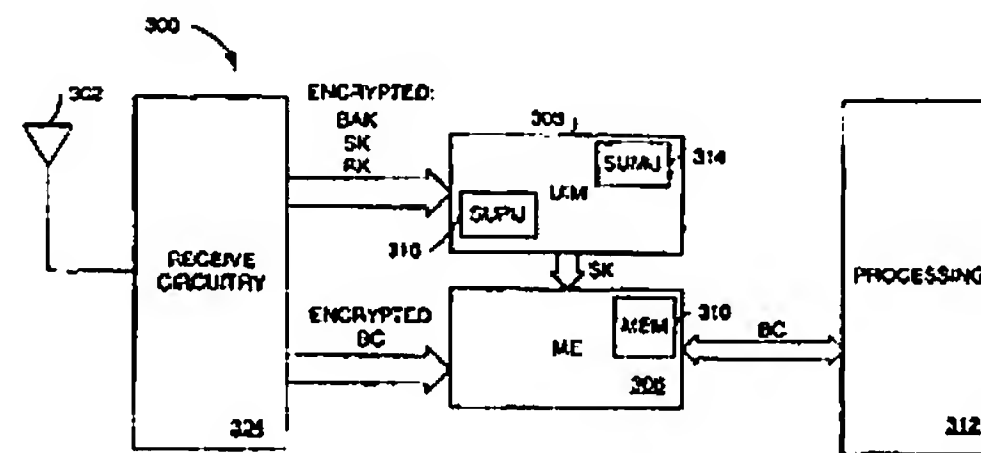
最終頁に続く

(54) 【発明の名称】 データ処理システムにおけるセキュリティのための方法および装置

(57) 【要約】

【解決手段】 安全な送信のための方法および装置。各ユーザには登録鍵が与えられる。長期間の更新されたブロードキャスト鍵は登録鍵を用いて暗号化され、定期的にユーザに与えられる。短期間の更新された鍵は、ブロードキャスト鍵を用いて暗号化され定期的にユーザに与えられる。次に、ブロードキャストは、短期間鍵を用いて暗号化され、ユーザは、短期間鍵を用いてブロードキャストメッセージを復号する。

【選択図】 図4



【特許請求の範囲】

【請求項 1】

下記を具備する安全送信のための方法：
送信の参加者に固有の登録鍵を決定する；
第 1 の鍵を決定する；
前記第 1 の鍵を前記登録鍵で暗号化する；
第 2 の鍵を決定する；
前記第 2 の鍵を前記第 1 の鍵で暗号化する；および
前記第 1 および第 2 の鍵を更新する。

【請求項 2】

更新はさらに下記を具備する、請求項 1 の方法：
第 1 の期間に従って、前記第 1 の鍵を更新する；および
第 2 の期間に従って、前記第 2 の鍵を更新する、前記第 2 の期間は前記第 1 の期間より短い。

【請求項 3】

更新はさらに下記を具備する、請求項 2 の方法：
更新された第 1 の鍵を前記登録鍵で暗号化する；および
更新された第 2 の鍵を前記更新された第 1 の鍵で暗号化する。

【請求項 4】

さらに下記を具備する請求項 2 の方法：
前記第 2 の鍵を用いて情報のブロードキャストストリームを暗号化する；および
前記暗号化された情報のブロードキャストストリームを送信する。

【請求項 5】

前記情報のブロードキャストストリームはビデオ情報から構成される、請求項 4 の方法。

【請求項 6】

前記情報のブロードキャストストリームは、インターネットプロトコルパケットから構成される、請求項 4 の方法。

【請求項 7】

さらに下記を具備する、請求項 3 の方法：
登録鍵情報メッセージを計算する；および
前記登録鍵情報メッセージを送信する。

【請求項 8】

さらに下記を具備する、請求項 7 の方法：
前記更新され、暗号化された第 1 の鍵に対応する第 1 の鍵情報メッセージを計算する；および
前記第 1 の鍵情報メッセージを送信する。

【請求項 9】

さらに下記を具備する、請求項 8 の方法：
前記更新され、暗号化された第 2 の鍵に対応する第 2 の鍵情報メッセージを計算する；および
前記第 2 の鍵情報メッセージを送信する。

【請求項 10】

さらに下記を具備する、請求項 1 の方法：
前記暗号化された第 1 の鍵を送信する；および
前記暗号化された第 2 の鍵を送信する。

【請求項 11】

下記を具備する、送信の安全な受信のための方法：
送信の参加者に固有の登録鍵を受信する；
第 1 の鍵を受信する；
前記第 1 の鍵を前記登録鍵で復号する；

10

20

30

40

50

第 2 の鍵を受信する；

前記第 2 の鍵を前記第 1 の鍵で復号する；

前記情報のブロードキャストストリームを受信する；および

前記第 2 の鍵を用いて前記情報のブロードキャストストリームを復号する。

【請求項 1 2】

下記をさらに具備する、請求項 1 1 の方法：

前記第 1 の鍵を安全メモリストレージユニットに記憶する；および

前記第 2 の鍵をメモリストレージユニットに記憶する。

【請求項 1 3】

下記をさらに具備する、請求項 1 1 の方法：

第 1 の鍵情報メッセージから前記第 1 の鍵を受信する；および

第 2 の鍵情報メッセージから前記第 2 の鍵を再生する。

【請求項 1 4】

下記をさらに具備する、請求項 1 1 の方法：

第 1 の期間に従って、前記第 1 の鍵を更新する；および

第 2 の期間に従って、前記第 2 の鍵を更新する。

【請求項 1 5】

ブロードキャストサービスオプションをサポートする無線通信システムにおいて、下記を具備する、インフラストラクチャエレメント：

受信回路；

鍵情報を復号するように動作する処理装置と、登録鍵を記憶するためのメモリストレージユニットを具備し、ブロードキャストメッセージを復号するために、短期間の鍵を再生するように動作するユーザー識別装置；および

前記ブロードキャストメッセージを復号するために前記短期間の鍵を利用するように適合された移動機器装置。

【請求項 1 6】

前記短期間の鍵は、前記ユーザー識別装置によって処理され、前記移動機器装置に渡される、請求項 1 5 のインフラストラクチャエレメント。

【請求項 1 7】

前記メモリストレージユニットは安全なメモリストレージユニットである、請求項 1 5 のインフラストラクチャエレメント。

【請求項 1 8】

前記メモリストレージユニットは、ブロードキャストアクセス鍵を記憶し、前記処理装置は、前記ブロードキャストアクセス鍵を用いて前記短期間の鍵を復号する、請求項 1 5 のインフラストラクチャエレメント。

【請求項 1 9】

前記短期間の鍵は、第 1 の頻度で更新される、請求項 1 8 のインフラストラクチャエレメント。

【請求項 2 0】

前記ブロードキャストアクセス鍵は、前記第 1 の頻度よりも少ない第 2 の頻度で更新される、請求項 1 9 のインフラストラクチャエレメント。

【請求項 2 1】

前記ブロードキャストサービスオプションはビデオサービスである、請求項 1 5 のインフラストラクチャエレメント。

【請求項 2 2】

下記を具備する無線通信システム：

送信の参加者に固有の登録鍵を決定する手段；

第 1 の鍵を決定する手段；

前記第 1 の鍵を前記登録鍵で暗号化する手段；

第 2 の鍵を決定する手段；

10

20

30

40

50

前記第 2 の鍵を前記第 1 の鍵で暗号化する手段；および
前記第 1 および第 2 の鍵を更新する手段。

【請求項 23】

下記を具備するインフラストラクチャエレメント：

送信の参加者に固有の登録鍵を受信する手段；

第 1 の鍵を受信する手段；

前記第 1 の鍵を前記登録鍵で復号する手段；

第 2 の鍵を受信する手段；

前記第 2 の鍵を前記第 1 の鍵で復号する手段；

情報のブロードキャストストリームを受信する手段；および

前記第 2 の鍵を用いて前記情報のブロードキャストストリームを復号する手段。

10

【請求項 24】

下記を具備するデジタル信号ストレージ装置：

送信の参加者に固有の登録鍵を受信するための第 1 の命令セット；

第 1 の鍵を受信するための第 2 の命令セット；

前記第 1 の鍵を前記登録鍵で復号するための第 3 の命令セット；

第 2 の鍵を受信するための第 4 の命令セット；

前記第 2 の鍵を前記第 1 の鍵で復号する第 5 の命令セット；

情報のブロードキャストストリームを受信するための第 6 の命令セット；および

前記第 2 の鍵を用いて前記ブロードキャストストリームを復号するための第 7 の命令セッ

20

ト。

【発明の詳細な説明】

【技術分野】

【0001】

背景

35 U. S. C. § 120 に基づく優先権の主張

【1001】この特許出願は、この発明の譲受人に譲渡され、参照することによりここに組み込まれる 2001 年 3 月 28 日に出願された米国仮出願第 60/279,970 の優先権を主張する。

【0002】

30

特許のための同時継続出願への参照

【1002】この発明は、米国特許商標局における以下の特許出願に関連する。

【0003】

この発明の譲受人に譲渡され、参照することにより、明示的にここに組み込まれ、代理人整理番号第 010439 を有する、ニコライ・リュウング(Nikolai Leung)による「無線通信システムにおけるオーバーヘッドメッセージングのための方法および装置」(METHOD AND APPARATUS FOR OVERHEAD MESSAGING IN A WIRELESS COMMUNICATION SYSTEM)と、

この発明の譲受人に譲渡され、参照することにより、明示的にここに組み込まれ、代理人整理番号第 010437 を有する、ニコライ・リュウング(Nikolai Leung)による「無線通信システムにおけるブロードキャストサービスオプションの帯域外の送信のための方法および装置」(METHOD AND APPARATUS FOR OUT-OF-BAND TRANSMISSION OF BROADCAST SERVICE OPTION IN A WIRELESS COMMUNICATION SYSTEM)と、

40

この発明の譲受人に譲渡され、参照することにより、明示的にここに組み込まれ、代理人整理番号第 010438 を有する、ニコライ・リュウング(Nikolai Leung)による「無線通信システムにおけるブロードキャストシグナリングのための方法および装置」(METHOD AND APPARATUS FOR BROADCAST SIGNALING IN A WIRELESS COMMUNICATION SYSTEM)と、この発明の譲受人に譲渡され、参照することにより、明示的にここに組み込まれ、代理人整理番号第 010498 を有する、レイモンド・スー(Raymond Hsu)による「無線通信システムにおける送信フレーミングのための方法および装置」(METHOD AND APPARATUS FOR TRANSMISSION FRAMING IN A WIRELESS COMMUNICATION SYSTEM)と、

50

この発明の譲受人に譲渡され、参照することにより、明示的にここに組み込まれ、代理人整理番号第010499を有する、レイモンド・スー(Raymond Hsu)による「無線通信システムにおけるデータ伝送のための方法および装置」(METHOD AND APPARATUS FOR DATA TRANSPORT IN A WIRELESS COMMUNICATION SYSTEM)および

この発明の譲受人に譲渡され、参照することにより、明示的にここに組み込まれ、代理人整理番号第010499を有する、レイモンド・スー(Raymond Hsu)による「無線通信システムにおけるヘッダ圧縮のための方法および装置」(METHOD AND APPARATUS FOR HEADER COMPRESSION IN A WIRELESS COMMUNICATION SYSTEM)に関連する。

【0004】

分野

【1003】この発明は、一般にデータ処理システムに関し、特に、データ処理システムにおけるセキュリティのための方法および装置に関する。

【背景技術】

【0005】

背景

【1004】通信システムを含む、データ処理および情報システムにおけるセキュリティは、説明責任、公正、正確さ、機密性、実現可能性並びに、他の所望の基準の過多に寄与する。暗号化または暗号法の一般的分野は、電子商取引、無線通信、放送に使用され、制限の無い

範囲のアプリケーションを有する。電子商取引において、暗号化は、詐欺行為を防止し、金融取引を検証するために使用される。データ処理システムにおいて、暗号化は、関係者のアイデンティティを検証するために使用される。暗号化は、また、ハッキングを防止し、ウェブページを保護し、機密文書へのアクセスを防止するために使用される。

【0006】

【1005】しばしば暗号システムと呼ばれる非対称暗号化システムはメッセージを暗号化および復号するのに同じ鍵(すなわち、秘密鍵)を使用する。ところが、非対称暗号化システムは、メッセージを暗号化するために第1の鍵(すなわち、公開鍵)を使用し、復号するのに、異なる鍵(すなわち、プライベート鍵)を使用する。非対称の暗号システムは、公開鍵暗号システムとも呼ばれる。対称暗号システムには、送信者から受信者への秘密鍵の安全な供給に問題がある。さらに、鍵またはその他の暗号機構が頻繁に更新される
とき、問題が存在する。データ処理システムにおいて、鍵を安全に更新する方法は、処理時間、メモリストレージ、および他の処理オーバーヘッドを招く。無線通信システムにおいて、鍵を更新することは、送信のために使用される可変帯域幅を使用する。

【0007】

【1006】従来技術は、移動局が暗号化された放送にアクセスすることができるために、大きなグループの移動局への鍵を更新するための方法を提供しない。それゆえ、データ処理システムにおいて、鍵を更新する安全で効果的な方法の必要性がある。さらに、無線通信システムにおいて、鍵を更新する安全で効果的な方法の必要性がある。

【発明の開示】

【課題を解決するための手段】

【0008】

【1007】ここに開示された実施の形態は、データ処理システムにおいて、安全性のための方法を供給することにより上述した必要性に対処する。

【0009】

【1008】一つの観点において、安全な送信のための方法は、送信の参加者に固有の登録鍵を決定し、第1の鍵を決定し、第1の鍵を登録鍵で暗号化し、第2の鍵を決定し、第2の鍵を第1の鍵で暗号化し、第1の鍵および第2の鍵を更新する。

【0010】

【1009】他の観点において、送信の安全な受信のための方法は、送信における参加者に固有の登録鍵を受信し、第1の鍵を受信し、第1の鍵を登録鍵で復号し、情報のブロー

10

20

30

40

50

ドキャストストリームを受信し、および第2の鍵を用いて情報のブロードキャストストリームを復号する。

【0011】

【1010】他の観点において、ブロードキャストサービスオプションを支持する無線通信システムは、受信回路を含むインフラストラクチャエレメントと、ブロードキャストメッセージを復号するために一時的な鍵を再生するように動作するユーザ識別装置と、およびブロードキャストメッセージを復号するために一時的な鍵を適用するように適合される移動機器装置を有する。ユーザ識別装置は、鍵情報を復号するように動作する処理装置と、登録鍵を記憶するメモリストレージユニットを含む。

【発明を実施するための最良の形態】

10

【0012】

【1024】「例示的な」という文言は、ここでは、もっぱら、「例、事例、または例証として取り扱う」ことを意味するために使用される。例示としてここに記載されるいかなる実施の形態も、他の実施の形態に対して、好適であるまたは有利であるとして必ずしも解釈されない。

【0013】

【1025】無線通信システムは、音声、データ等のような種々のタイプの通信を提供するために広く展開されている。これらのシステムは、符号分割多重アクセス(CDMA)、時分割多重アクセス(TDMA)あるいはその他の変調技術に基づくことができる。CDMAシステムは、システム容量の増加を含む、他のタイプのシステムに対してある利点を供給する。

20

【0014】

【1026】システムは、ここでは、IS-95標準と呼ばれる、「デュアルモード広帯域スペクトラム拡散セルラシステムのためのTIA/EIA-IS-95B移動局-基地局互換標準のような1つ以上の標準をサポートするように設計することができる。この標準は、ここでは、3GPPと呼ぶ「第三世代パートナーシッププロジェクト」という名前がつけられた共同事業体により提供され、ここでは、W-CDMA標準と呼ぶ、ドキュメント番号3G TS 25.211、3G TS 25.212、3G TS 25.213および3G TS 25.214、3G TS 25.302を含むドキュメントのセットに具現化される。W-CDMA標準は、ここでは、3GPP2と呼ぶ「第三世代パートナーシッププロジェクト2」という名前がつけられた共同事業体、および正式にはIS-2000 MCと呼ばれ、ここでは、cdma2000標準と呼ぶTR-45.5により提供される。上で引用した標準は参照することによりここに明示的に組み込まれる。

30

【0015】

【1027】各標準は特に、基地局から移動局への送信のためのデータの処理および逆もまた同様の処理を定義する。例示実施の形態として、以下の議論は、cdma2000システムと一致するスペクトル拡散通信システムを考慮に入れる。他の実施の形態は、別の標準/システムを包含することができる。さらに他の実施の形態は、ここに開示したセキュリティ方法を暗号システムを用いたいかなるタイプのデータ処理にも適用することができる。

40

【0016】

【1028】暗号システムは、メッセージを変装させる方法であり、それにより特定のグループのユーザがそのメッセージを抽出することができる方法である。図1Aは基本暗号システムを図解する。暗号法は暗号システムを作成し使用する技術である。暗号解析は、メッセージへのアクセスが許された特定のグループのユーザ内にいないときに、暗号システムを破る、すなわちメッセージを受信し理解する技術である。原文は、平文メッセージまたは平文と呼ばれる。暗号化されたメッセージは暗号文と呼ばれ、暗号化は、平文を暗号文に変換するための何らかの手段を含む。復号は暗号文を平文に変換する手段、すなわち、原メッセージを再生する手段を含む。図1Aに示すように、平文メッセージは、暗号文を形成するために暗号化される。次に、暗号文が受信され、平文を再生するために復号

50

される。平文および暗号文という用語は一般にデータのことであるが、暗号化の概念は、デジタルの形態で提供されるオーディオデータおよびビデオデータを含むいかなるデジタル情報にも適用できる。ここに提供されるこの発明の記載は、暗号法の技術に一致する平文および暗号文という用語を用いるが、これらの用語は他の形態のデジタル通信を排除しない。

【0017】

【1029】暗号システムは秘密に基づいている。あるグループのエンティティは、このグループ外のエンティティが特に大きな容量のリソースを伴わずに、秘密を得ることができなければ、秘密を共有する。この秘密は、エンティティのグループ間のセキュリティ関連づけの役割があると言われている。

【0018】

【1030】暗号システムはアルゴリズムの集合であり得、各アルゴリズムにラベルが付され、ラベルは鍵と呼ばれる。しばしば暗号システムと呼ばれる対称暗号化システムはメッセージを暗号化および復号するために同じ鍵（すなわち、秘密鍵）を用いる。対称暗号化システムは図1Bに図解され、暗号化と復号の両方が同じプライベート鍵を使用する。

【0019】

【1031】それにひきかえ、非対称暗号化システムは、メッセージを暗号化するために第1の鍵（すなわち、公開鍵）を用い、復号するために異なる鍵（すなわち、プライベート鍵）を用いる。図1Cは非対称暗号化システムを図解し、1つの鍵が暗号化のために提供され、第2の鍵が復号のために提供される。非対称暗号化システムは公開鍵暗号システムとも呼ばれる。公開鍵はメッセージを暗号化するために発行され利用可能であるが、公開鍵で暗号化されたメッセージを復号するためにプライベート鍵のみを使用することができる。

【0020】

【1032】送り手から受取人に秘密鍵を安全に供給する際に、対称暗号システムに問題が存在する。1つの解決において、情報を供給するのにクーリエを用いることができる。または、より効率的で信頼できる解決法は、以下に述べる、Rivest, Shamir, および Adleman (RSA) により定義される公開鍵暗号システムのような、公開鍵暗号システムを用いることである。RSAシステムは、以下にさらに詳細に説明される、Pretty Good Privacy (PGP) と呼ばれる、良く知られる安全ツールに使用される。例えば、もともと記録された暗号システムは、アルファベット内の各文字を n だけシフトすることにより、平文内の文字を変更した。この場合、 n は所定の定数の整数値である。そのようなスキームにおいて、「A」は「D」に置換される等、所定の暗号化スキームはいくつかの異なる値の n を組み込むことができる。この暗号化スキームにおいて、「 n 」は鍵である。意図された受取人には暗号文を受信する前に、暗号化スキームが提供される。このようにしてその鍵を知っているものだけが、暗号文を復号して平文を再生できなければならない。しかしながら、暗号の知識を用いてその鍵を計算することにより、意図しない受取人が暗号文を途中で捕まえ、暗号文を復号することができ、安全性に問題がある。

【0021】

【1033】より複雑で高機能の暗号システムは、意図しないパーティからの傍受および復号を阻止する戦略的な鍵を採用する。古典的な暗号システムは暗号関数 E および復号関数 D を以下のように採用する。

【0022】

平文 P に対して $D_K (E_K (P)) = P$

(1)

【1034】公開鍵暗号システムにおいて、 E_K は K から計算される公知の「公開鍵」 Y から容易に計算される。 Y は発行されるので、誰でもメッセージを暗号化することができる。復号関数 D_K は公開鍵 Y から計算されるが、プライベート鍵の知識を有する場合のみである。プライベート鍵が無ければ、意図しない受取人はそのように発生された暗号文を復号することはできない。このようにして、 K を発生した受取人のみがメッセージを復号することができる。

10

20

30

40

50

【0023】

【1035】RSAは、Rivest, Shamir,およびAdlemanにより定義された公開鍵暗号システムである。一例として、平文を 2^{512} までの正の整数として考える。鍵は4部分(p , q , e , d)からなり、 p は256ビット素数として与えられ、 q は258ビット素数として与えられ、 d および e は $(p-1)(q-1)$ で割り切れる $(de-1)$ を有する大数である。さらに、暗号関数を以下のように定義する：

$$E_K(P) = P^e \bmod pq, D_K(C) = C^d \bmod pq \quad (2)$$

【1036】 E_K は対 (pq, e) から容易に計算されるが、対 (pq, e) から D_K を計算する知られた簡単な方法はない。それゆえ、 K を発生する受取人は (pq, e) を発行することができる。受取人がメッセージを読むことが出来る唯一の受取人であるとき、その受取人に秘密のメッセージを送信することは可能である。

10

【0024】

【1037】PGPは対象暗号化および非対称暗号化からの特徴を結合する。図1Dおよび1Eは平文メッセージが暗号化され、再生されるPGP暗号システム50を図解する。図1Dにおいて、平文メッセージは、モデムの送信時間とディスクスペースを節約するために圧縮される。圧縮は、暗号化および復号処理に他のレベルの変換を追加することにより暗号法の安全性を強化する。殆どの暗号解読技術は、暗号を解読するために平文に発見されたパターンを利用する。圧縮は平文の中のこれらのパターンを低減し、それにより暗号解読に対する抵抗を高める。留意すべき点は、一実施の形態は、短すぎて圧縮できない、またはうまく圧縮しない平文または他のメッセージを圧縮しない。

20

【0025】

【1038】PGPは次に、一度だけの秘密鍵であるセッション鍵を作る。この鍵は、タイプしている間のマウスおよびキーストロークのランダムな移動のようなランダムイベントから発生することができる乱数である。セッション鍵は、平文を暗号化するための安全な暗号アルゴリズムと共に機能し、暗号文を生じる。データが暗号化されると、次にセッション鍵は受取人の公開鍵に暗号化される。この公開鍵暗号化されたセッション鍵は、暗号文とともに受取人に送信される。

【0026】

【1039】図1Eに示すように、復号の場合、PGPの受取人のコピーはプライベート鍵を用いて、一時的なセッション鍵を再生する。PGPは次にそれを用いて、一般的に暗号化された暗号文を復号する。暗号方法の組合せは、公開鍵暗号化の利便性と対称暗号化の速度を利用する。対称暗号化は、公開鍵暗号化より一般に非常に早い。公開鍵暗号化は、それはそれで、鍵配布およびデータ送信の問題への解決を与える。組み合わせることにより、安全性を損なうことなく、性能と鍵配布が改良される。

30

【0027】

【1040】鍵は、特定の暗号文を形成するために、暗号アルゴリズムとともに機能する値である。鍵は、基本的に非常に大きな数である。鍵サイズはビットで測定される。公開鍵暗号法において、安全性は鍵サイズとともに増加するが、公開鍵サイズと対称暗号化プライベート鍵サイズは、一般に関係無い。公開鍵とプライベート鍵は数学的に関連するが、公開鍵のみを与えられて、プライベート鍵を派生するには困難性が生じる。十分な時間と計算能力を与えられれば、プライベート鍵の派生は可能であり、鍵サイズの選択を重要な安全性の問題にする。目標は、迅速に処理するために、鍵サイズを十分小さく維持しながら、安全である大きな鍵を持つことである。さらなる考慮すべき事柄は、予期される阻止する人である。特に、第三者へのメッセージの重要性は何か、およびどの程度のリソースを第三者が復号しなければならないかである。

40

【0028】

【1041】より大きな鍵は、長期間、暗号法的に安全であろう。鍵は暗号化された形態で記憶される。PGPは特に、鍵を2つのファイルに記憶する。すなわち、公開鍵のためのファイルと、プライベート鍵のためのファイルである。これらのファイルはキーホルダーと呼ばれる。アプリケーションにおいて、PGP暗号システムは、目的とする受取人の

50

公開鍵を送信者の公開キーホルダーに付加する。送信者のプライベート鍵は、送信者のプライベートキーホルダーに記憶される。

【0029】

〔1042〕上であげられた例に記載するように、暗号化および復号のために使用される鍵を配布する方法は、複雑にすることができる。「鍵交換問題」は最初に、送り手と受け手の両方がそれぞれ暗号化および復号を実行できるように、および双方向通信に対して、送り手と受け手がメッセージを暗号化および復号の両方を行なうことができるように、鍵が交換されることを確実にすることを含む。さらに、鍵交換は、意図しない第三者による妨害を排除するように行なわれることが望ましい。最後にさらなる考察は、メッセージが意図された送り手によって暗号化され、第三者によるものではないことを受け取り手に保証を与える認証である。プライベート鍵交換システムにおいて、鍵は秘密に交換され、成功する鍵交換および正当な認証に改良された安全性を与える。留意すべきは、プライベート鍵暗号化スキームは、暗黙のうちに認証を与えるという点である。プライベート鍵暗号システムにおける基礎的前提は、意図された送り手のみが、意図された受取り手に配布されるメッセージを暗号化することができる鍵を持つであろうということである。公開鍵暗号の方法は鍵交換問題の重要な観点を解決する、特に、鍵交換中に立ち聞きする人がいたとしても解析を困難にするけれども、鍵交換に関するすべての問題を解決するわけではない。特に、鍵は、「公の知識」（特にRSAの場合）なので、認証を与えるその他の機構が望まれる。（メッセージを暗号化するために十分な）鍵のみの所有は、送り手の特定の固有のアイデンティティの証拠にもならないし、それだけで、受取人のアイデンティティを確立するのに十分な復号鍵を持っていることにもならない。

10

20

【0030】

〔1043〕1つの解決は、リストされた鍵が、実際に、時として、信頼されている当局、認証局、1/3第三者預託代理人と呼ばれる与えられたエンティティの鍵であることを保証する鍵配布機構を開発することである。当局は、一般には、実際には、鍵を発生せず、送り手と受け手の参考のために、維持され、公表される、鍵のリストおよび関連するアイデンティティが正しく妥協がないことを保証する。他の方法は、互いの鍵を配布して追跡し、非公式の配布された方法に信頼を置くユーザに依存する。RSAでは、暗号化されたメッセージに加えて、アイデンティティの証拠を送信したい場合、署名がプライベート鍵で暗号化される。受け手は、送り手のみが秘密鍵の使用により平文を暗号化できたというように、情報を復号することを検証するために、逆にRSAアルゴリズムを使用することができる。一般に、暗号化された「署名」は秘密メッセージの固有の数学的「要約」から構成される「メッセージダイジェスト」である（署名が複数のメッセージにわたり固定的であるなら、一度知った以前の受け取り手は誤って使用することも有り得る）。このようにして、メッセージの送り手のみがそのメッセージに対して正当な署名を発生することができ、受取り手に対して認証することができる。

30

【0031】

〔1044〕メッセージダイジェストはしばしば暗号ハッシュ関数を用いて計算される。暗号ハッシュ関数は、入力の高さに関係なく、入力から（固定のビット数で）値を計算する。暗号ハッシュ関数の特性はこうである：出力が与えられると、その出力を生じる入力を決定することが計算的に困難である。暗号ハッシュ関数の一例は、米商務省の連邦情報処理規格公報、米商務省技術標準局により公布された「安全ハッシュ規格」FIPS PUB 180-1に記載されたSHA-1である。

40

【0032】

〔1045〕図2は多数のユーザをサポートし、この発明の少なくともいくつかの観点および実施の形態を実施することができる通信システム100の一例である。システム100において、送信をスケジュールするためにいろいろなアルゴリズムおよび方法のいずれかを使用することができる。システム100は多数のセル102A乃至102Gに対して通信を供給する。それらのセルの各々は、それぞれ対応する基地局104A乃至104Gによりサービスされる。例示実施の形態において、基地局104のいくつかは、複数の受

50

信アンテナを有し、他は単一の受信アンテナを有する。同様に、基地局104のいくつかは複数の送信アンテナを有し、他は、単一の送信アンテナを有する。送信アンテナと受信アンテナの組合せに制限は無い。それゆえ、基地局が複数の送信アンテナと単一の受信アンテナを有することも可能であるし、または複数の受信アンテナと単一の送信アンテナを有することも可能であるし、または、単一のまたは複数の送信アンテナおよび受信アンテナを有することも可能である。

【0033】

【1046】カバー領域内の端末106は固定（すなわち、静止している）していてもよいし、または移動していてもよい。図2に示すように、種々の端末106がシステム全体に分散している。各端末106は、ソフトハンドオフが採用されるかどうか、または端末が複数の基地局から複数の送信を（同時にまたは順次に）受信するように設計され動作するかどうかに応じて、いつなんどきでも、ダウンリンクおよびアップリンクを介して一つおよび恐らくそれ以上の基地局104と通信する。CDMA通信システムのソフトハンドオフは、技術的によく知られており、この発明の譲受人に譲渡された米国特許第5,101,501（発明の名称：「CDMAセルラ電話システムにソフトハンドオフを供給するための方法およびシステム」(METHOD AND SYSTEM FOR PROVIDING A SOFT HANDOFF IN A CDMA CELLULAR TELEPHONE SYSTEM)に詳細に記載されている。

【0034】

【1047】ダウンリンクは基地局から端末への送信を呼び、アップリンクは端末から基地局への送信を呼ぶ。例示実施の形態において、端末106のいくつかは、複数の受信アンテナを有し、他は唯ひとつの受信アンテナを有する。図2において、基地局104Aはダウンリンクを介してデータを端末106Aおよび106Jに送信し、基地局104Bは端末106Bおよび106Jにデータを送信し、基地局104Cは端末106Cにデータを送信する、等である。

【0035】

【1048】無線データ送信の増えている需要および無線通信技術を介して利用可能なサービスの拡張により特定のデータサービスが開発された。そのようなサービスの1つは高データレート（HDR）と呼ばれる。HDRサービスの例示は、「HDR仕様書」と呼ばれる「E1A/T1A-IS856cdma2000高レートパケットデータ大気インターフェース仕様書」に提案されている。HDRサービスは一般に無線通信システムにおいて、データの packets を送信する効率的な方法を提供する音声通信システムへの重畳である。送信されたデータ量および送信回数が増えるにつれ、無線送信のために利用可能な限られた帯域幅は、重要なリソースになる。それゆえ、利用可能な帯域幅の使用を最適化する通信システムにおける送信をスケジューリングする効率的で公正な方法のための必要性がある。例示実施の形態において、図2に示すシステム100はHDRサービスを有するCDMAタイプシステムと一致する。

【0036】

【1049】一実施の形態によれば、システム100は、高速ブロードキャストサービス（HSBS）と呼ばれる高速マルチメディアブロードキャストサービスをサポートする。HSBSの例示アプリケーションは映画、スポーツイベント、等のビデオストリーミング（video streaming）である。HSBSサービスは、インターネットプロトコル（IP）に基づくパケットデータサービスである。例示実施の形態に従って、サービスプロバイダはそのような高速ブロードキャストサービスの利用可能性をユーザに示す。HSBSサービスを望むユーザは、サービスを受信するために申し込み、広告、ショート管理システム（SMS）、無線アプリケーションプロトコル（WAP）等を介して、ブロードキャストサービススケジュールを発見することができる。モバイルユーザは移動局（MSs）と呼ばれる。基地局（BSs）は、HSBS関連パラメータをオーバーヘッドメッセージで送信する。MSがブロードキャストセッションを受信したいとき、MSはオーバーヘッドメッセージを読み適切な構成を学習する。次に、MSはHSBSチャネルを含む周波数に同調し、ブロードキャストサービスコンテンツを受信する。

10

20

30

40

50

【0037】

【1050】考察されるサービスは、高速マルチメディアブロードキャストサービスである。このサービスは、この文書においては、高速ブロードキャストサービス（HSBS）と呼ばれる。そのような例の1つは、映画、スポーツイベント等のビデオストリーミングである。このサービスは、インターネットプロトコル（IP）に基づくパケットデータサービスであると思われる。

【0038】

【1051】サービスプロバイダーは、そのような高速ブロードキャストサービスの利用可能性をユーザに示すであろう。そのようなサービスを望む移動局ユーザは、このサービスを受信することを申し込むであろう、そして広告、SMS、WAP等を介してブロードキャストサービススケジュールを発見することができる。基地局は、オーバーヘッドメッセージでブロードキャストサービス関連パラメータを送信するであろう。そのブロードキャストセッションを聞きたいと願う移動局は、これらのメッセージを読み、適当な構成を決定し、高速ブロードキャストチャネルを含む周波数に同調し、ブロードキャストサービスコンテンツの受信を開始する。

【0039】

【1052】無料アクセス、制御アクセス、および部分制御アクセスを含む、HSBSのためのいくつかの可能な申し込み／歳入モデルがある。無料アクセスの場合、サービスを受信するために移動局による申し込みは必要無い。BSはコンテンツを暗号化せずに放送し、関心のある移動局は、そのコンテンツを受信することができる。サービスプロバイダーのための歳入は、そのブロードキャストチャネル内に送信することができる広告を介して発生することができる。例えば、次の映画のカットされた場面を送信することができ、それに対して、スタジオがサービスプロバイダーに支払うであろう。

【0040】

【1053】制御アクセスの場合、MSユーザはそのサービスに対して申し込みをし、ブロードキャストサービスを受信するために対応する料金を払う。申し込んでいないユーザは、

HSBSサービスを受信することができない。制御アクセスは、申し込んだユーザのみがコンテンツを復号できるように、HSBS送信／コンテンツを暗号化することにより、達成することができる。これは、無線の暗号化鍵交換手続きを使用することができる。このスキームは強い安全性を供給し、サービスの盗難を防止する。

【0041】

【1054】部分制御アクセスと呼ばれるハイブリッドアクセススキームは、間欠性の暗号化されない広告送信を伴って暗号化される、加入ごとのサービスとしてHSBSサービスを提供する。これらの広告は、暗号化されたHSBSサービスへの申し込みを強化するように意図することができる。これらの暗号化されていないセグメントのスケジュールは外部手段を介してMSに知らせしめることができる。

【0042】

【1055】無線通信システム200は図3に図解される。ビデオおよびオーディオ情報は、コンテンツサーバー（CS）201によりパケット化されたデータサービスネットワーク（PDSN）202に供給される。ビデオおよびオーディオ情報はテレビプログラミングまたは無線送信から得られる。情報はIPパケットのようなパケット化されたデータとして供給される。PDSN202はアクセスネットワーク（AN）内への配布のためにIPパケットを処理する。図解するように、ANは、複数のMS206と通信するBS204を含むシステムの一部として定義される。PDSN202は、BS204に接続される。HSBSサービスの場合、BS204は、PDSN202から情報のストリームを受信し、指定されたチャネルを介して、システム200内の加入者に情報を提供する。アクセスを制御するために、PDSN202に提供される前にCS201によりコンテンツが暗号化される。申し込んだユーザには、復号鍵が与えられるので、IPパケットを復号することができる。

10

20

30

40

【0043】

【1056】図4は、図3のMS206同様のMS300の詳細図である。MS300は、受信回路304に接続されたアンテナ302を有する。MS300は、図3のBS204と同様のBS（図示せず）からの送信を受信する。MS300はユーザ識別モジュール（UIM）308とモバイル機器（ME）306を含む。受信回路は、UIM308とME306に接続される。UIM308はHSBS送信の安全性のために検証手続きを印加し、種々の鍵をME306に供給する。ME306は、処理装置312に接続することができる。ME306は、これに限定されないが、HSBSコンテンツストリームの復号を含む実質的な処理を実行する。ME306は、メモリストレージユニット、MEM310を含む。例示実施の形態において、ME306処理（図示せず）におけるデータおよびMEメモリストレージユニットにおけるデータは、限られたリソースの使用により非加入者により容易にアクセス可能であり、それゆえ、ME306は安全でないとされる。ME306を通過した情報またはME306により処理された情報は、短い期間だけ、安全に秘密を維持する。それゆえ、ME306と共有する鍵のような秘密の情報をしばしば変更することが望ましい。

10

【0044】

【1057】UIM308は長期間秘密を維持しなければならない（暗号鍵のような）秘密の情報を記憶し処理するように委託される。UIM308は安全な装置なので、その中に記憶された秘密は、システムがその秘密情報をしばしば変更することを必ずしも要求する必要が無い。UIM308は、安全UIM処理装置（SUPU）316と呼ばれる処理装置と、安全であると信頼されている安全UIMメモリ装置（SUMU）314と呼ばれるメモリストレージ装置を含む。UIM308内において、SUMU314は、その情報への不正アクセスの意欲を減退させるように秘密情報を記憶する。秘密情報がUIM308から得られるなら、そのアクセスは極めて大量のリソースを必要とするであろう。また、UIM308内において、SUPU316は、UIM308に対して外部にある値に関して計算を実行し、および／またはUIM308に対して内部にある値に関して計算を実行する。計算の結果は、SUMU314に記憶してもよいしまたはME306に送られる。SUPU316を用いて実行された計算は、極めて大量のリソースを有したエンティティによりUIM308から得ることができるのみである。同様に、SUMU314内に記憶される（しかし、ME306への出力ではない）ように指定されるSUPU316からの出力は、権限のない妨害が極めて大量のリソースを必要とするように設計される。一実施の形態において、UIM308は、MS300内の固定装置である。留意すべきは、UIM308内の安全メモリおよび処理に加えて、UIM308はまた、電話番号、eメールアドレス情報、ウェブページまたはURLアドレス情報、および／またはスケジューリング関数等を含む情報を記憶する非安全メモリおよび処理（図示せず）も含んでいる。

20

30

【0045】

【1058】代わりの実施の形態は、脱着可能なおよび／または再プログラム可能なUIMを供給することができる。例示実施の形態において、SUPU316は、HSBSのブロードキャストコンテンツの暗号化を可能にするような、セキュリティと鍵の手続きを越える機能に対しては意味のある、処理能力を有していない。代わりの実施の形態は、より強い処理能力を有するUIMを実施してもよい。

40

【0046】

【1059】UIMは特定のユーザと関連し、主に、MS300が、携帯電話ネットワークへのアクセスのように、ユーザに与えられた特権の資格があるかどうかを検証するために主に使用される。それゆえ、ユーザはMS300よりもUIM308に関連している。同じユーザが複数のUIM308に関連することができる。

【0047】

【1060】ブロードキャストサービスは、どのように鍵を、加入したユーザに配布するかを決定する問題に面している。特定の時間にブロードキャストコンテンツを復号するために、MEは現在の復号鍵を知らなければならない。サービスの盗難を回避するために、

50

復号鍵は頻繁に、例えば分毎に変更しなければならない。これらの復号鍵は短期鍵（S K）と呼ばれる。S Kは短い期間、ブロードキャストコンテンツを復号するために使用され、従って、S Kは、ユーザに対して、若干の固有の金銭的価値を持つものと見なすことができる。例えば、この固有の金銭的価値は、登録コストの一部であり得る。加入者のメモリストレージユニット、MEM 310から非加入者がS Kを得るコストがS Kの固有の金銭的価値を越えたと仮定する。すなわちS Kを（違法に）得るコストが報酬を越え、利益が無い。従って、メモリストレージユニット、MEM 310においてS Kを保護する必要が無い。しかしながら、秘密鍵が、S Kの寿命よりも長い寿命を有するなら、この秘密鍵を（違法に）得るコストは報酬よりも少ない。この状況において、メモリストレージユニット、MEM 310からそのような鍵を得る利点がある。それ故、理想的には、メモリストレージユニット、MEM 310は、S Kの寿命よりも長い寿命を有した秘密を記憶しないであろう。

10

【0048】

【1061】S Kを種々の加入者装置に配布するためにCS（図示せず）により使用されるチャンネルは安全でないと考えられる。それゆえ、与えられたS Kを配布するとき、CSは、加入していないユーザからS Kの値を隠す技術を使用することを望む。さらに、CSは、短い時間フレーム内でそれぞれのMEにおいて処理するために、複数の多数の加入者の各々に、S Kを配布する。鍵送信の周知の安全な方法は低速で多数の鍵の送信を必要とし、一般には、所望の基準に対して実現可能でない。例示実施の形態は、非加入者が復号鍵を得ることができないような方法で、短い時間フレーム内で多数の加入者のセットに復号鍵を配布する実現可能な方法である。

20

【0049】

【1062】例示実施の形態において、MS 300は無線通信システムにおいてHSBSをサポートする。HSBSへのアクセスを得るために、ユーザは登録し、サービスに加入しなければならない。申し込みがイネーブルになると、種々の鍵が周期的に更新される。登録プロセスにおいて、CSとUIM 308は、ユーザとCSとの間のセキュリティアソシエーション（security association）としての機能を果たす登録鍵（RK）に同意する。従って、CSは、UIMに、RKで暗号化されたさらなる秘密情報を送信することができる。RKは、UIM 308において、秘密として維持され、与えられたUIMに対して固有である。すなわち、各ユーザには異なるRKが割当てられる。登録プロセスだけでは、HSBSにユーザアクセスを与えない。上で述べたように、登録の後、ユーザはサービスを申し込む。申し込みのプロセスにおいて、CSはUIM 308に共通ブロードキャストアクセス鍵（BAK）の値を送信する。CSはMS 300に、特にUIM 308に、UIM 308に固有RKを用いて暗号化されたBAKの値を送信する。UIM 308は、RKを用いた暗号化されたバージョンからオリジナルBAKの値を再生することができる。BAKはCSと申し込んだユーザのグループとの間のセキュリティアソシエーションとしての機能を果たす。従って、CSはS Kを派生するために、UIM 308において、BAKと結合されるS K情報（SK）と呼ばれるデータをブロードキャストする。次に、UIM 308はS KをME 306に渡す。このようにして、CSは、S Kの新しい値を申し込んだユーザのMEに効率的に配布することができる。

30

40

【0050】

【1063】次の段落は、登録プロセスを詳細に述べる。ユーザが与えられたCSに登録すると、UIM 308とCS（図示せず）はセキュリティアソシエーションを構築する。すなわち、UIM 308とCSは秘密鍵RKに同意する。RKは各UIM 308に固有である。しかし、ユーザが複数のUIMを有するなら、これらのUIMは、CSの政策に応じて同じRKを共有するかもしれない。この登録はユーザがCSにより提供されるブロードキャストチャンネルに申し込むと、生じる、または申し込みの前に生じることができる。単一のCSは複数のブロードキャストチャンネルを提供することができる。CSは、ユーザをすべてのチャンネルに対して同じRKに関連づけるように選択することができ、または、各チャンネルに対して登録するようにユーザに要求するように選択することができ、および同

50

じユーザに対して、異なるチャネル上の異なるR Kを関連づけるように選択することができる。複数のC Sは、同じ登録鍵を使用するように選択することができ、各C Sに対して異なるR Kを登録し取得するように要求することができる。

【0051】

【1064】このセキュリティアソシエーションを構築するための2つの共通シナリオは、(3GPPにおいて使用される)認証鍵同意(A K A)方法およびI P s e cにおいて使用されるインターネット鍵交換方法(I K E)を含む。いずれにしても、U I MメモリユニットS U M U 3 1 4はA鍵と呼ばれる秘密鍵を含む。一例として、A K A方法が記載される。A K A方法において、A鍵は、U I Mおよび信頼されている第三者(T T P)にのみ知られている秘密である：T T Pは1つ以上のエンティティから構成してもよい。T T Pは一般にユーザが登録される移動サービスプロバイダである。C SとT T Pとの間のすべての通信は安全であり、そして、C SはT T Pがブロードキャストサービスへの不正アクセスを支援しないであろうことを委託する。ユーザが登録すると、C SはT T Pにユーザがそのサービスに登録することを望んでいることを知らせ、そして、ユーザの要求の検証を行なう。T T Pは、A鍵からR Kを計算するための(暗号ハッシュ関数に類似した)関数を使用するとともに、登録鍵情報(R K I)と呼ばれるさらなるデータを使用する。T T Pは安全なチャネルを介して、この依頼に関係の無い他のデータと共にR K、R K IをC Sに渡す。C Sは、R K IをM S 3 0 0に送る。受信回路3 0 4は、R K IをU I M 3 0 8に渡し、恐らく、R K IをM E 3 0 6に渡す。U I M 3 0 8は、R K Iと、U I MメモリユニットS U M U 3 1 4に記憶されているA鍵とからR Kを計算する。R KはU I MメモリユニットS U M U 3 1 4に記憶され、M E 3 0 6に直接供給されない。代替の実施の形態は、I K Eシナリオまたはその他の方法を用いてR Kを確立する。R KはC SとU I M 3 0 8とのセキュリティアソシエーションとして機能する。

【0052】

【1065】A K A方法において、R KはC S、U I MおよびT T Pの間で秘密共有される。それゆえ、ここで使用するように、A K A方法は、C SとU I Mとの間のセキュリティアソシエーションは、暗黙のうちにT T Pを含むことを意味する。C SはT T Pにブロードキャストサービスへの不正アクセスを支援しないように委託するので、セキュリティアソシエーションへのT T Pの包含は、セキュリティ違反とは考えない。上述したように、鍵がM E 3 0 6と共有されるなら、その鍵をしばしば変更することが望ましい。これは、メモリストレージユニット、M E M 3 1 0に記憶された非加入者アクセス情報のリスクによるものであり、従って、制御されたまたは部分的に制御されたサービスへのアクセスを可能にする。M E 3 0 6は、S K(ブロードキャストコンテンツを復号するために使用される鍵情報)をメモリストレージユニット、M E M 3 1 0に記憶する。C SはS Kを計算するために申し込んだユーザのための情報を十分に送信しなければならない。申し込んだユーザのM E 3 0 6がこの情報からS Kを計算することができたなら、S Kを計算するために必要なさらなる情報は秘密にすることはできない。この場合、申し込んでないユーザのM E 3 0 6もこの情報からS Kを計算できたと仮定する。それゆえ、S Kの値は、C SとS U M U 3 1 4により共有される秘密鍵を用いてS U P U 3 1 6において計算しなければならない。C SとS U M U 3 1 4は、R Kの値を共有するが、各ユーザはR Kという固有の値を有する。C SがR Kのすべての値を用いてS Kを暗号化し、これらの暗号化された値を各申し込んだユーザに送信するには時間が十分でない。その他の技術が必要である。

【0053】

【1066】以下の段落は、申し込みプロセスを詳細に記載する。安全な情報S Kの効率的な配布を保障するために、C Sは周期的に共通ブロードキャストアクセス鍵(B A K)を各加入者U I M 3 0 8に周期的に配布する。各加入者に対して、C Sは、対応するR Kを用いてB A Kを暗号化し、B A K I(B A K情報)と呼ばれる値を得る。C Sは、対応するB A K Iを加入者ユーザのM S 3 0 0に送信する。例えば、B A Kは、各M Sに対応するR Kを用いて暗号化されたI Pパケットとして送信することができる。例示実施の形

10

20

30

40

50

態において、BAKIはIPSecパケットである。例示実施の形態において、BAKIは、鍵としてRKを用いて暗号化されたBAKを含むIPSecである。RKはユーザ毎の鍵であるので、CSは、BAKを各加入者個々に送信しなければならない。従って、BAKは、ブロードキャストチャンネルを介して送信されない。MS300はBAKIをUIM308に渡す。SUPU316は、SUMU314に記憶されたRKの値およびBAKIの値を用いてBAKを計算する。次に、BAKの値は、SUMUに記憶される。例示実施の形態において、BAKIは、MS300にBAKIをUIM308に渡すように命令し、およびUIM308にBAKIを暗号化するためにRKを使用するように命令するセキュリティパラメータインデックス(SPI)を含む。

【0054】

10

【1067】BAKを更新するための期間は、顕著なオーバーヘッドを被ることなく、CSがBAKを各加入者個々に送信可能にするのに十分であることが望まれる。ME306は、長時間にわたり、秘密を維持するように委託されていないので、UIM308はBAKをME306に供給しない。BAKは、CSとHSBSサービスの加入者のグループとの間のセキュリティアソシエーションとして機能する。

【0055】

【1068】以下の段落は、成功した申し込みプロセスに続いてどのようにSKが更新されるかについて述べる。BAKを更新するための各期間内において、SKがブロードキャストチャンネルに配布される短期間の間隔が供給される。SKがBAKとSKIから決定できるように、2つの値SKとSKI(SKI情報)を決定するためにCSは暗号関数を使用する。例えば、SKIは、鍵として、BAKを用いたSKの暗号であり得る。例示実施の形態において、SKIは、鍵としてBAKを用いて暗号化されるSKを含むIPSecパケットである。あるいは、SKは、ブロックSKIおよびBAKの連結に暗号ハッシュ関数を適用する結果であり得る。

20

【0056】

【1069】SKIのある部分は予測できるかもしれない。例えば、SKIの一部は、このSKIが有効であるシステムタイム時間から派生することができる。SKI__Aの名称である、この部分は、ブロードキャストサービスの一部としてMS300に送信される必要はない。SKIの残りである、SKI__Bは予測することができない。SKI__Bは、ブロードキャストサービスの一部としてMS300に送信される必要がない。MS300はSKI__AおよびSKI__BからSKIを再構築し、SKIをUIMに供給する。SKIはUIM308内で再構築してもよい。SKIの値は、各新しいSKに対して変更しなければならない。従って、SKI__Aおよび/またはSKI__Bは新しいSKを計算するとき変更しなければならない。CSはSKI__Bをブロードキャスト送信のためにBSに送る。BSは、アンテナ302により検出される、SKI__Bをブロードキャストし、受信回路304に渡す。受信回路304は、SKI__BをMS300に供給し、MS300はSKIを再構築する。MS300はSKIをUIM308に供給し、UIM308は、SUMU314に記憶されたBAKを用いてSKを取得する。次に、SKは、UIM308によりME306に供給される。ME306は、SKをメモリストレージユニット、MEM310に記憶する。ME306は、SKを用いてCSから受信したブロードキャスト送信を復号する。

30

40

【0057】

【1070】例示実施の形態において、SKIはまた、SKIをUIM308に渡すようにMS300に命令し、SKIを復号するためにBAKを使用するようにUIM308に命令するセキュリティパラメータインデックス(SPI)を含む。復号の後、UIM308は、SKをME306に渡し、ME306はSKを用いてブロードキャストコンテンツを復号する。

【0058】

【1071】CSとBSはSKI__Bが送信されるときのある基準に合意する。CSはSKを頻繁に変更することにより、各SKにおける固有の金銭的価値を低減したいかもしれ

50

ない。この状況において、SK1__Bデータを変更したいという要望は、利用可能な帯域幅を最適化することに対してバランスされる。SK1__Bは、ブロードキャストチャンネル以外のチャンネルに送信することができる。ユーザーがブロードキャストチャンネルに「同調」すると、受信回路は、「制御チャンネル」からブロードキャストチャンネルを見つける情報を得る。ユーザーがブロードキャストチャンネルに「同調」するとき、迅速なアクセスを可能にすることが望ましいかもしれない。これは、ME306が短期間にSK1を得ることを必要とする。ME306はすでにSK1__Aを知っているであろうけれども、BSは、SK1__Bを短期間にME300に供給しなければならない。例えば、BSは、（ブロードキャスト情報を見つけるための情報と共に）制御チャンネルに頻繁にSK1__Bを送信することができ、または、ブロードキャストチャンネルに頻繁にSK1__Bを送信することができる。BSがSK1__Bの値をしばしば「リフレッシュ」すればする程、MS300はブロードキャストメッセージにアクセスすることができる。あまりにも頻繁にSK1__Bデータを送信することは、制御チャンネルまたはブロードキャストチャンネル内の受け入れられない量の帯域幅を使用してもよいので、SK1__Bデータをリフレッシュする要望は、利用可能な帯域幅を最適化することに対してバランスされる。

10

【0059】

【1072】この段落は、ブロードキャストコンテンツの暗号と送信について述べる。CSは現在のSKを用いてブロードキャストコンテンツを暗号化する。例示実施の形態はアドバンスドエンクリプションスタンダード(Advanced Encryption Standard)(AES)暗号アルゴリズムのような暗号化アルゴリズムを採用する。例示実施の形態において、暗号化された内容は、エンカプシュレーションセキュリティペイロード(ESP)移送モードに従って、IPsecパケットにより運ばれる。IPsecパケットは、受信したブロードキャストコンテンツを復号するために、現在のSKを使用するようにME306に命令するSPI値も含む。暗号化されたコンテンツは、ブロードキャストチャンネルを介して送られる。

20

【0060】

【1073】受信回路304は、RK1およびBAK1を直接UIM308に供給する。さらに、受信回路は、SK1を得るために、SK1__Aと結合されるMS300の適当な部分にSK1__Bを供給する。SK1は、MS300の関連する部分によりUIM308に供給される。UIM308は、RK1およびA鍵からRKを計算し、RKを用いてBAK1を復号して、BAKを取得し、SK1およびBAKを用いてSKを計算し、ME306により使用するためのSKを発生する。ME306は、SKを用いてブロードキャストコンテンツを復号する。例示実施の形態のUIM308は、ブロードキャストコンテンツをリアルタイムに復号する十分な能力がないので、それゆえ、SKはブロードキャストコンテンツを復号するために、ME306に渡される。

30

【0061】

【1074】図5は例示実施の形態に従う鍵RK、BAKおよびSKの送信と処理を図解する。図解するように、MS300はRK1を受信し、それをUIM308に渡す。SUPU316はRK1およびA鍵を用いてRKを計算し、RKをUIMメモリストレージSUMU314に記憶する。MS300は、UIM308に固有なRK値を用いて暗号化されたBAKを含むBAK1を周期的に受信する。暗号化されたBAK1は、SUPU316により復号されBAKを再生する。BAKはUIMメモリストレージSUMU314に記憶される。MS300はさらに周期的にSK1__Bを受信する。SK1__BはSK1__Aと結合し、SK1を形成する。SUPU316はSK1およびBAKからSKを計算する。SKはブロードキャストコンテンツを復号するためにME306に供給される。

40

【0062】

【1075】例示実施の形態において、CS鍵は、必ずしも暗号化され、MSに送信される必要はない。CSは代わりの方法を使用してもよい。各MSに送信するためにCSにより発生された鍵情報は、MSが鍵を計算するのに十分な情報を供給する。図6のシステム350に図解するように、RKはCSにより発生されるが、RK情報(RK1)はMSに

50

送信される。CSはUIMがRKを派生するのに十分な情報を送信する。ここでは、CSからの送信された情報からRKを派生するために所定の関数を使用される。RKIは、d1のラベルがつけられた所定の公開関数を用いて、A—鍵と、システム時間のような他の値からオリジナルのRKをMSが決定するのに十分な情報を含む。

【0063】

[1076] $RK = d1(A\text{—}鍵, RKI)$ (3)

[1077] 例示実施の形態において、関数d1は暗号タイプの関数を定義する。一実施の形態によれば、RKIは以下のように決定される。

【0064】

[1078] $RK = SHA'(A\text{—}鍵 \parallel RKI)$ (4)

[1079] 「 \parallel 」は、A—鍵とRKIを含むブロックの連結を示し、 $SHA'(X)$ は、入力Xを与えられたセキュアハッシュアルゴリズムSHA-1の出力の最後の128ビットを示す。代替の実施の形態において、RKは、以下のように決定される。

【0065】

[1080] $RK = AES(A\text{—}鍵, RKI)$ (5)

[1081] $AES(X, Y)$ は、128ビットA—鍵を用いた128ビットブロックRKIの暗号化を示す。AKAプロトコルに基づくさらなる実施の形態において、RKは、3GPP鍵発生関数f3の出力として決定される。この場合、RKIは、RANDの値と、標準により定義されるAMFとSQNの適切な値を含む。

【0066】

[1082] RKの異なる値を有する複数のユーザは、BAKの同じ値を計算するので、BAKは異なる方法で取り扱われる。CSはBAKを決定するためにいかなる技術を使用してもよい。しかしながら、特定のUIM308に関連するBAKIの値は、UIM308に関連する固有のRKに基づいてBAKの暗号でなければならない。SUPU316は以下の式に従いd2のラベルがつけられた関数に従って、SUMU314内に記憶されたRKを用いてBAKIを復号する。

【0067】

[1083] $BAK = d2(BAKI, RK)$ (9)

[1084] 代替の実施の形態において、CSはRKを用いてBAKに復号プロセスを適用することによりBAKIを計算し、SUPU316はRKを用いてBAKIに暗号化プロセスを適用することによりBAKを得る。これは、CSがBAKを暗号化し、SUPU316がBAKIを復号するのと等価であると考えられる。代替の実施の形態は、図6に図解する鍵の組合せに加えてまたは鍵の組合せの代わりに、いかなる数の鍵の組合せも実施することができる。

【0068】

[1085] SKはRKに対する方法と同様な方法で取り扱われる。最初のSKIは、SKI—AおよびSKI—B(SKI—BはCSからMSに送信される情報である)から派生される。d3のラベルが付けられた所定の関数を用いて、以下の式に従って、SKIおよび(SUMU314に記憶される)BAKを派生する。

【0069】

[1086] $SK = d3(BAK, SKI)$ (6)

[1087] 一実施の形態において、関数d3は暗号タイプの関数を定義する。例示実施の形態において、SKは以下のように計算される。

【0070】

[1088] $SK = SHA(BAK \parallel SKI)$ (7)

[1089] 一方、他の実施の形態において、SKは以下のように計算される。

【0071】

[1090] $SK = AES(BAK, SKI)$ (8)

[1091] ブロードキャストメッセージに対してセキュリティを供給する方法は、図7A—7Dに図解される。図7Aはステップ402において、加入者がCSと登録を交渉す

10

20

30

40

50

る登録プロセス400を図解する。ステップ404における登録は、UIMに固有のRKを供給する。UIMは、ステップ406において、セキュアメモリユニット(SUMU)にRKを記憶する。図7BはCSとMSとの間の加入処理を図解する。ステップ422において、CSは、BAK期間T1にBAKを発生する。BAKはBAK期間T1の間中有効であり、BAKは周期的に更新される。ステップ424において、CSは、BAK期間T1の間UIMにブロードキャストコンテンツ(BC)をアクセスする権限を与える。ステップ426において、CSは、各加入者のための各個々のRKを用いてBAKを暗号化する。暗号化されたBAKはBAKIと呼ばれる。次に、CSはステップ428においてBAKIをUIMに送信する。UIMは、ステップ430において、BAKIを受信し、RKを用いて復号を実行する。復号されたBAKIはもともと発生されたBAKを生じる。UIMはステップ432において、BAKをSUMUに記憶する。次に、UIMは、ブロードキャストセッションを受信し、暗号化されたブロードキャスト(BC)の復号にBAKを適用することによりBCをアクセスすることができる。

10

【0072】

【1092】図7Cは、ブロードキャストサービスをサポートする無線通信システムにおいて、セキュリティ暗号化のための鍵を更新する方法を図解する。この方法は図7Eに与えられた期間実施する。BAKは期間T1を有し、周期的に更新される。タイマーt1はBAKが計算されるとき開始され、T1でタイムアウトする。SK__RANDと呼ばれるSKを計算するために変数が使用される。SK__RANDは期間T2を有して周期的に更新される。タイマーt2は、SK__RANDが発生されると開始され、T2においてタイムアウトする。一実施の形態において、SKはさらに、T3の期間を有して周期的に更新される。タイマーt3は、各SKが発生されると、開始され、T3でタイムアウトする。SK__RANDは、CSで発生され、周期的にMSに供給される。以下に詳細に記載するように、MSとCSはSK__RANDを用いてSKを発生する。

20

【0073】

【1093】第1のタイマーt1は、BAKの適用できる値が更新されると、リセットされる。2つのBAK更新間の時間の長さはBAK更新期間である。例示実施の形態において、BAKの更新期間は1ヶ月である。しかしながら、代替の実施の形態は、システムの最適な動作に要望されるいかなる期間または、種々のシステム基準を満足するために要望されるいかなる期間をも実施することができる。

30

【0074】

【1094】図7Cを続けると、方法440は、ステップ442において、タイマーt2をイニシャライズし、SK__REG期間T2を開始する。CSはSK__RANDを発生し、ステップ444において、システムの全体に渡って、送信のために送信回路にその値を供給する。タイマーt3はステップ446においてイニシャライズされ、SK期間T3を開始する。次に、CSは、ステップ448において、現在のSKを用いてBCを暗号化する。暗号化された産物はEBCであり、CSはシステム内の送信のために送信回路にEBCを供給する。判断ひし形450においてタイマーt2が満了するなら、処理は、ステップ442に戻る。t2はT2よりも小さいけれども、判断ひし形452において、タイマーt3が満了するなら、処理はステップ446に戻り、そうでなければ、処理は450に戻る。

40

【0075】

【1095】図7DはブロードキャストサービスをアクセスするMSの動作を図解する。方法460は、最初に、ステップ462において、タイマーt2およびt3をCSにおける値と同期させる。ステップ464において、MSのUIMは、CSにより発生されたSK__RANDを受信する。ステップ466において、UIMは、SK__RAND、BAK、および時間測定値を用いてSKを発生する。UIMは、SKをMSのMEに渡す。次に、ステップ468において、UIMは、SKを用いて受信したEBCを復号し、もともとのBCを抽出する。ステップ470において、タイマーt2が満了すると、処理はステップ462に戻る。タイマーt2はT2より小さいけれども、ステップ472において、タ

50

イマー t 3 が満了するなら、ステップ 474 において、タイマー t 3 がイニシャライズされ、466に戻る。

【0076】

【1096】特定の BAK 更新期間に、ユーザがブロードキャストサービスを申し込むと、CS は (RK で暗号化された BAK に対応する) 適切な情報 BAK I を送信する。これは、一般に、BAK 更新期間の開始前に、またはこの BAK 更新期間に MS が最初にブロードキャストチャンネルに同調するとき、生じる。これは、種々の基準によって、MS または CS により開始することができる。複数の BAK I を同時に送信し復号してもよい。

【0077】

【1097】留意すべきは、BAK 更新期間の満了が差し迫ったとき、次の BAK 更新期間に MS が申し込んだなら、MS は CS から更新された BAK を要求することができる点である。代替の実施の形態において、最初のタイマー t 1 は CS により使用され、タイマーの満了時に、すなわち、BAK 更新期間が満足されたとき、CS は BAK を送信する。

10

【0078】

【1098】留意すべきは、BAK 更新期間にユーザが BAK を受信することが可能であり、この場合、例えば、BAK 更新が月毎に実行されるなら、加入者は、月の途中でサービスに加入するという点である。さらに、すべての加入者が一時に更新されるように、BAK 更新および SK 更新のための期間は同期させることができる。

【0079】

20

【1099】図 8A は、例示実施の形態に従って、無線通信システムにおける登録プロセスを図解する。CS 502 は、各加入者、すなわち、MS 512 と交渉し、特定の RK を加入者の各々に発生する。RK は各 MS の UIM 内の SUMU ユニットに供給される。図解するように、CS 502 は、UIM₁ 512 内の SUMU₁ 510 に記憶される RK₁ を発生する。同様に、CS 502 は、それぞれ UIM₂ 522 内の SUMU₂ 520 および UIM_N 532 内の SUMU_N 530 に記憶される RK₂ および RK_N を発生する。

【0080】

【1100】図 8B は、システム 500 内の申し込みプロセスを図解する。CS 502 はさらに複数のエンコーダ 504 を含む。エンコーダ 504 の各々は、固有の RKs の 1 つと、CS 502 において発生された BAK 値を受信する。各エンコーダ 504 の出力は、特に加入者のために符号化された BAK I である。BAK I は、UIM₁ 512 のような各 MS の UIM において受信される。各 UIM は、UIM₁ 512 の SUP I₁ 514 および SUMU₁ 510 のような SUP U と SUMU を含む。SUP U は、UIM の RK の適用により BAK を再生するデコーダ 516 のようなデコーダを含む。このプロセスは各加入者において反復される。

30

【0081】

【1101】鍵管理および更新は、図 8C に図解される。図 8C において、CS は SK __ RAND の値を発生するために関数 508 を利用する。SK __ RAND は、SK を計算するために、CS および MS により使用される暫定的値である。特に、関数 508 は BAK 値、SK __ RAND、および時間係数を利用する。図 8C に図解する実施の形態は、いつ SK を更新するかを決定するためにタイマーを利用するけれども、代替の実施の形態は、周期的な更新を与えるための代替の測定値、例えば、エラーまたは他のイベントの発生を使用してもよい。CS は、SK __ RAND を加入者の各々に供給し、この場合、各 UIM に常駐する関数 518 は、CS の関数 508 と同じ関数を利用する。関数 518 は、SK __ RAND、BAK、およびタイマー値に機能し、ME₁ 540 の MEM₁ 542 のような ME 内のメモリロケーションに記憶される SK を発生する。

40

【0082】

【1102】図 8D は、登録および申し込みの後の BC の処理を図解する。CS 502 は、現在の SK を用いて BC を符号化し、EBC を発生するエンコーダ 560 を含む。次に

50

、E B Cは、加入者に送信される。各M Sは、S Kを用いてE B CからB Cを抽出するエンコーダ5 4 4のようなエンコーダを含む。

【0083】

【1103】この発明は、一方向のブロードキャストサービスをサポートする無線通信システムの例示実施の形態に関して記載したけれども、上で述べた暗号化方法および鍵管理は、さらに、マルチキャストタイプブロードキャストシステムを含む他のデータ処理システムに適用可能である。さらに、この発明は、安全でないチャネルを介して、安全な情報の単一の送信に複数の加入者がアクセスするいかなるデータ処理システムにも適用可能である。

【0084】

【1104】情報および信号は、いろいろな異なる、技術および技法のいずれかを用いて表すことができることを当業者は理解する。例えば、上述の記載の全体に渡って参照してもよいデータ、命令、コマンド、情報、信号、ビット、記号、およびチップは有利に、電圧、電流、電磁波、磁界、磁性粒子、光学界、光学粒子、またはそれらのいずれかの組合せにより表現することができる。

【0085】

【1105】当業者はさらに、ここに開示した実施の形態に関連して記載した種々の実例となる論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェアまたは両方の組合せで実施できることを理解するであろう。このハードウェアとソフトウェアの互換性を明瞭に説明するために、種々の実例となる部品、ブロック、モジュール、回路、およびステップが一般にそれらの機能性の観点から上に記載された。そのような機能性がハードウェアまたはソフトウェアとして実現されるかは特定のアプリケーションおよび全体のシステムに課せられた設計制約に依存する。熟達した職人は、各特定のアプリケーションに対して記載した機能性を変形した方法で実施することができるが、そのような実施の判断は、この発明の範囲を逸脱するものとして解釈されるべきでない。

【0086】

【1106】ここに開示された実施の形態に関連して記載された種々の実例となる論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタルシグナルプロセッサ(D S P)、特定用途向け集積回路(A S I C)、フィールドプログラマブルゲートアレイ(F P G A)または他のプログラマブル論理装置、ディスクリートゲートまたはトランジスタロジック、ディスクリートハードウェアコンポーネント、またはここに記載した機能を実行するように設計されたいずれかの組合せを用いて実施または実行することができる。汎用プロセッサは、マイクロプロセッサであってよいが、別の方法では、プロセッサは、いずれかの一般的なプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであってよい。プロセッサはまた、計算装置の組合せとしても実施できる。例えば、D S Pとマイクロプロセッサの組合せ、複数のマイクロプロセッサ、D S Pコアと協力した1つ以上のマイクロプロセッサまたはいずれかの他のそのような構成として実施することもできる。

【0087】

【1107】ここに開示された実施の形態に関連して記載された方法またはアルゴリズムは、ハードウェアにおいて、プロセッサにより実行されるソフトウェアモジュールにおいて、または両者の組合せにおいて直接具現化することができる。ソフトウェアモジュールは、R A Mメモリ、フラッシュメモリ、R O Mメモリ、E P R O Mメモリ、E E P R O Mメモリ、レジスタ、ハードディスク、脱着可能ディスク、C D - R O M、または技術的に知られているその他のいずれかの形態の記憶媒体に存在することができる。例示記憶媒体は、プロセッサに接続される。そのようなプロセッサは記憶媒体から情報を読み出し、記憶媒体に情報を書き込むことができる。別の方法では、記憶媒体は、プロセッサに集積可能である。プロセッサと記憶媒体はA S I Cに存在してもよい。A S I Cはユーザ端末に存在してもよい。別の方法では、プロセッサと記憶媒体はユーザ端末内のディスクリート

10

20

30

40

50

コンポーネントとして存在してもよい。

【0088】

【1108】開示した実施の形態の上述の記載は当業者がこの発明を製作または使用することを可能にするために提供される。これらの実施の形態に対する種々の変更は当業者には容易に明白であろう、そしてここに定義される包括的原理は発明力の使用なしに他の実施の形態に適用可能である。従って、この発明は、ここに示した実施の形態に限定されることを意図したものではなく、ここに開示した原理と新規な特徴に一致する最も広い範囲が許容されるべきである。

【図面の簡単な説明】

【0089】

10

【図1A】 【1011】 図1Aは暗号システムの図である。

【図1B】 【1012】 図1Bは、対称暗号システムの図である。

【図1C】 【1013】 図1Cは非対称暗号システムの図である。

【図1D】 【1014】 図1DはPGP暗号システムの図である。

【図1E】 【1015】 図1Eは、PGP復号システムの図である。

【図2】 【1016】 図2は、多数のユーザをサポートするスペクトラム拡散通信システムの図である。

【図3】 【1017】 図3はブロードキャスト送信をサポートする通信システムのブロック図である。

【図4】 【1018】 図4は、無線通信システムにおける移動局のブロック図である。

20

【図5】 【1019】 図5は、ブロードキャストアクセスを制御するために使用される移動局内の鍵の更新を記載するモデルである。

【図6】 【1020】 図6はUIM内の暗号動作を記載するモデルである。

【図7A】 【1021】 図7Aはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティ暗号化を実施する方法を図解する。

【図7B】 【1021】 図7Bはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティ暗号化を実施する方法を図解する。

【図7C】 【1021】 図7Cはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティ暗号化を実施する方法を図解する。

【図7D】 【1021】 図7Dはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティ暗号化を実施する方法を図解する。

30

【図7E】 【1022】 図7Eはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティオプションの鍵更新期間のタイミング図である。

【図8A】 【1023】 図8Aはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティ暗号化方法のアプリケーションを図解する。

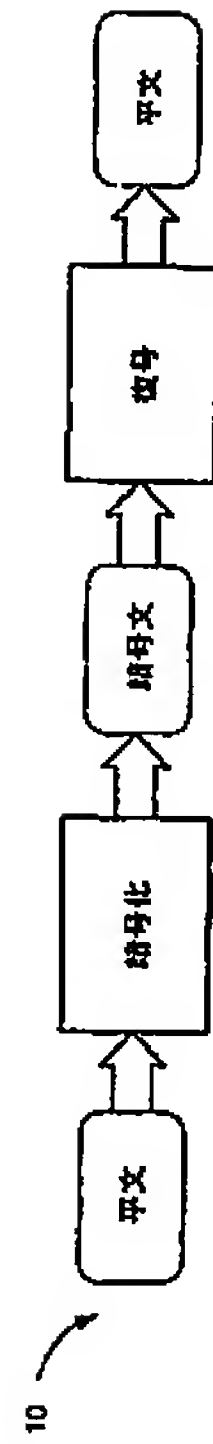
【図8B】 【1023】 図8Bはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティ暗号化方法のアプリケーションを図解する。

【図8C】 【1023】 図8Cはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティ暗号化方法のアプリケーションを図解する。

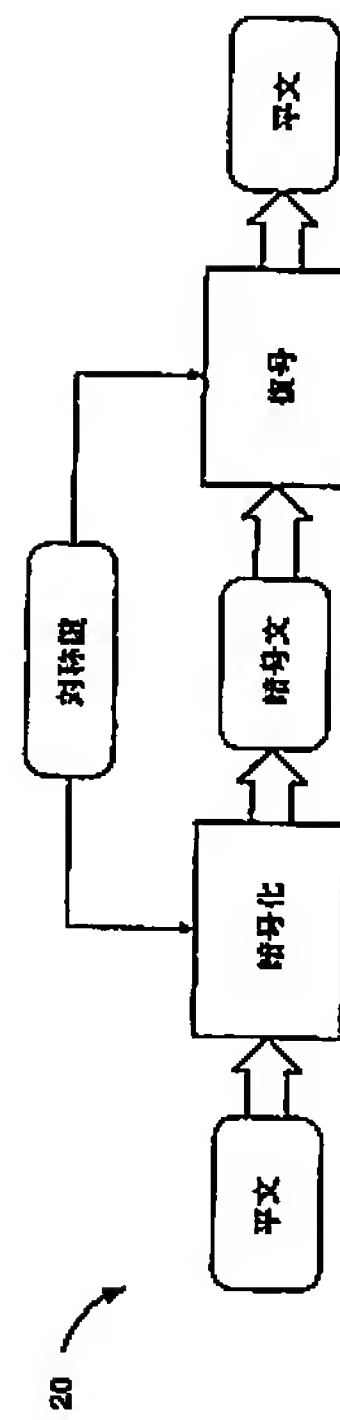
【図8D】 【1023】 図8Dはブロードキャスト送信をサポートする無線通信システムにおいて、セキュリティ暗号化方法のアプリケーションを図解する。

40

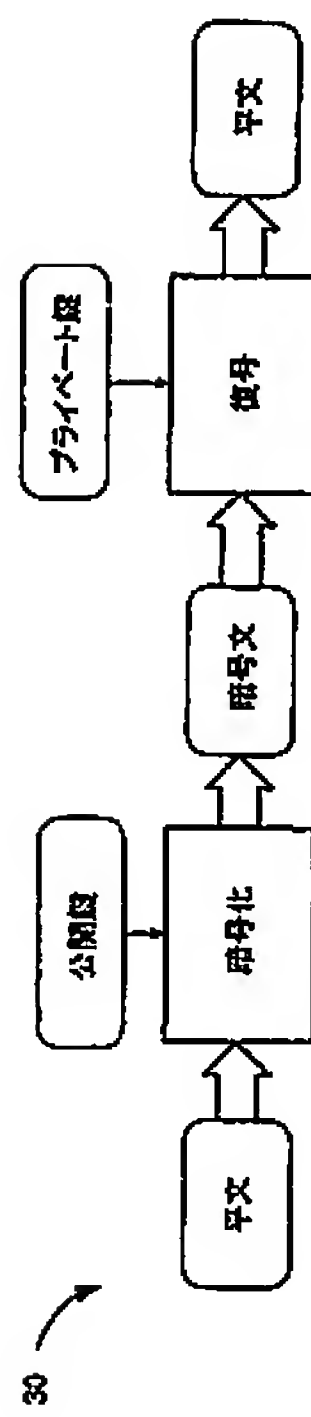
【図 1 A】



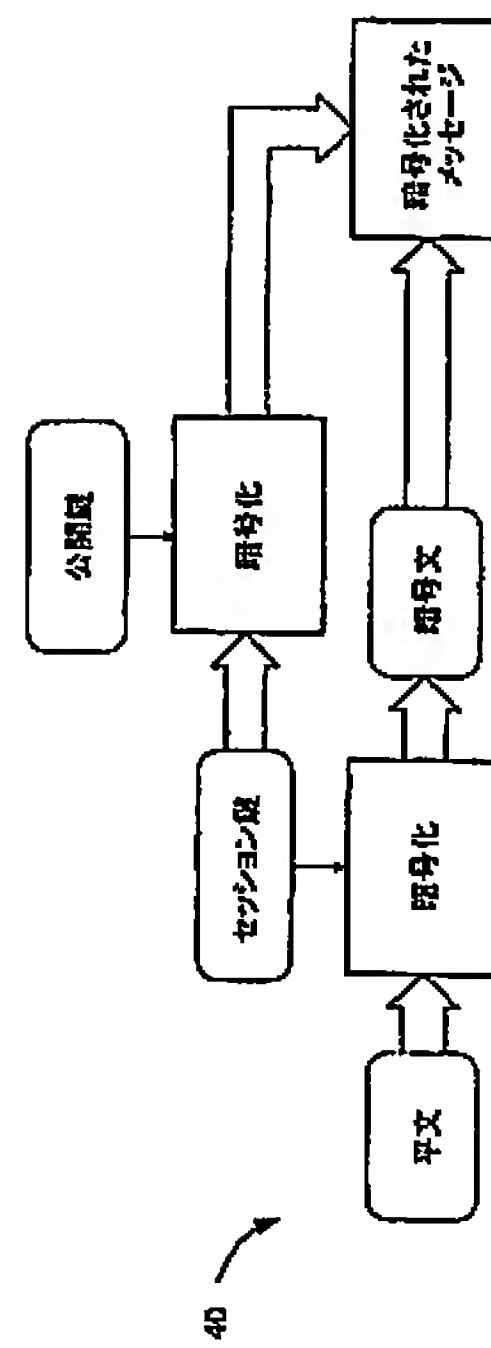
【図 1 B】



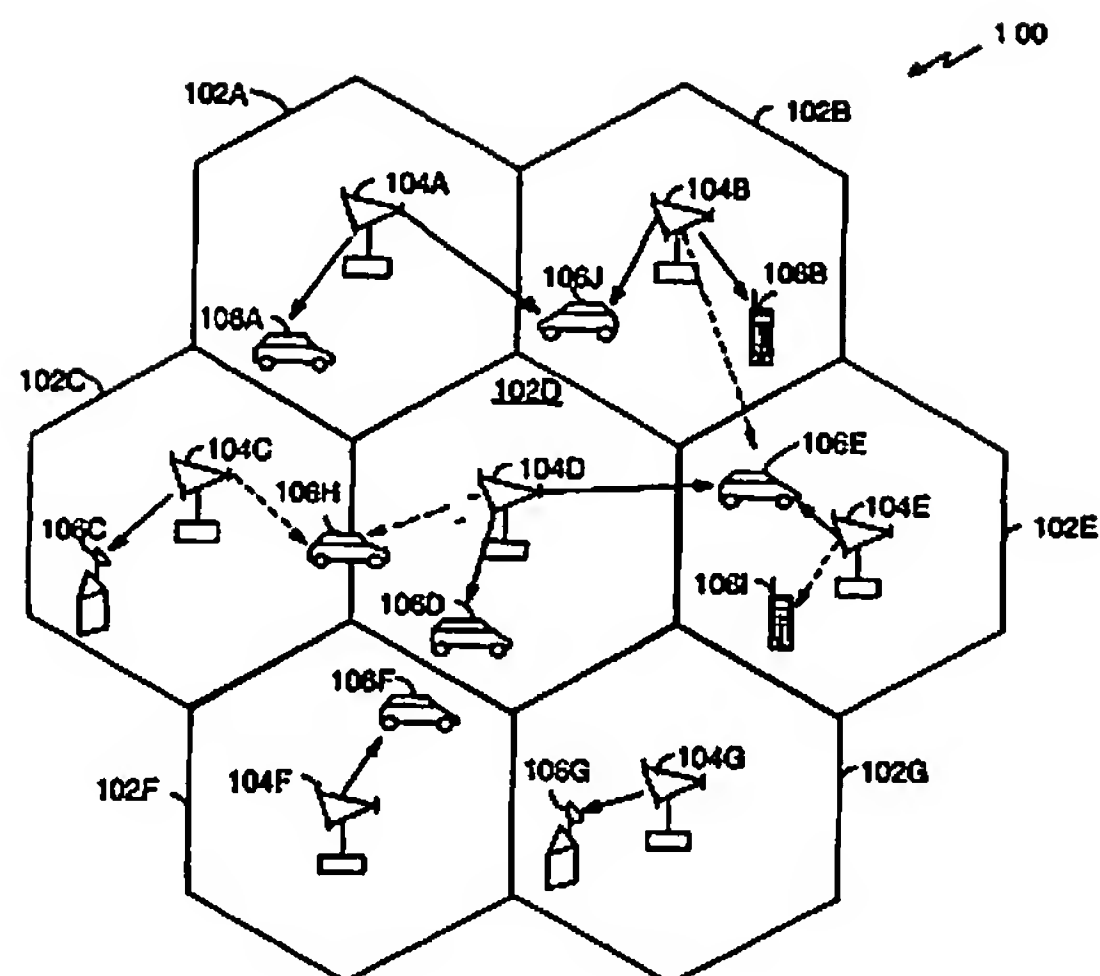
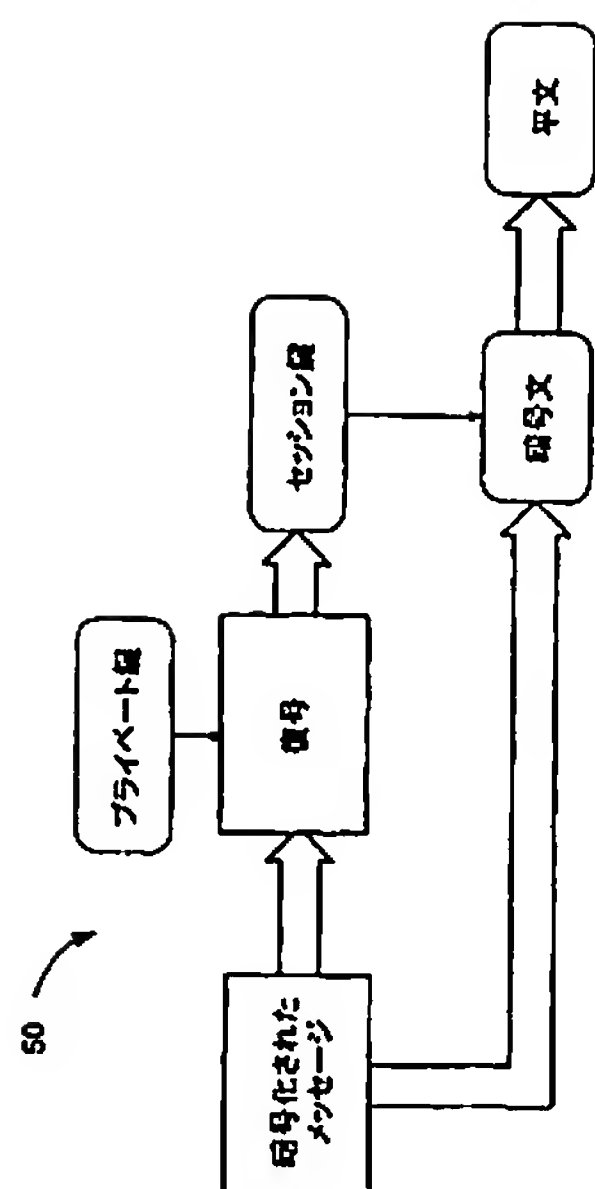
【図 1 C】



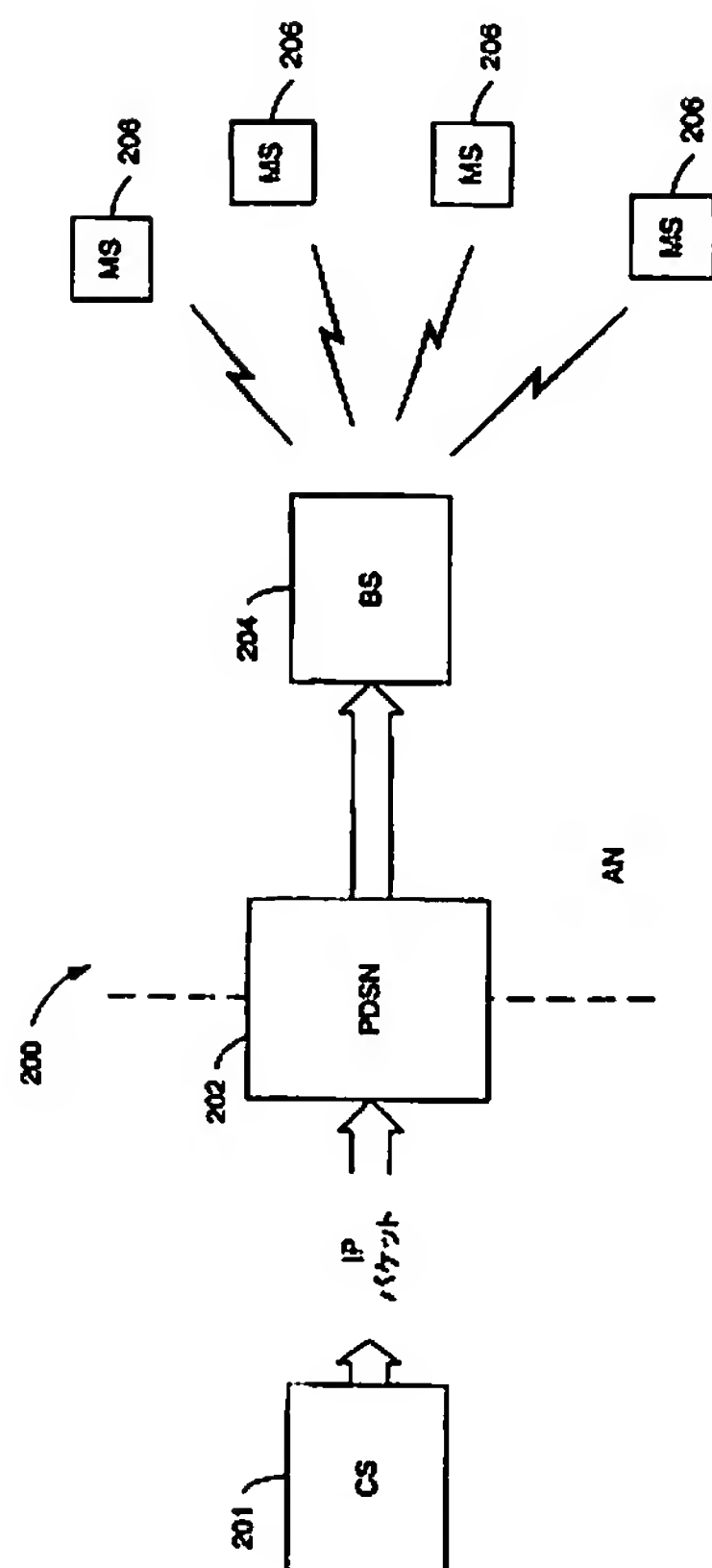
【図 1 D】



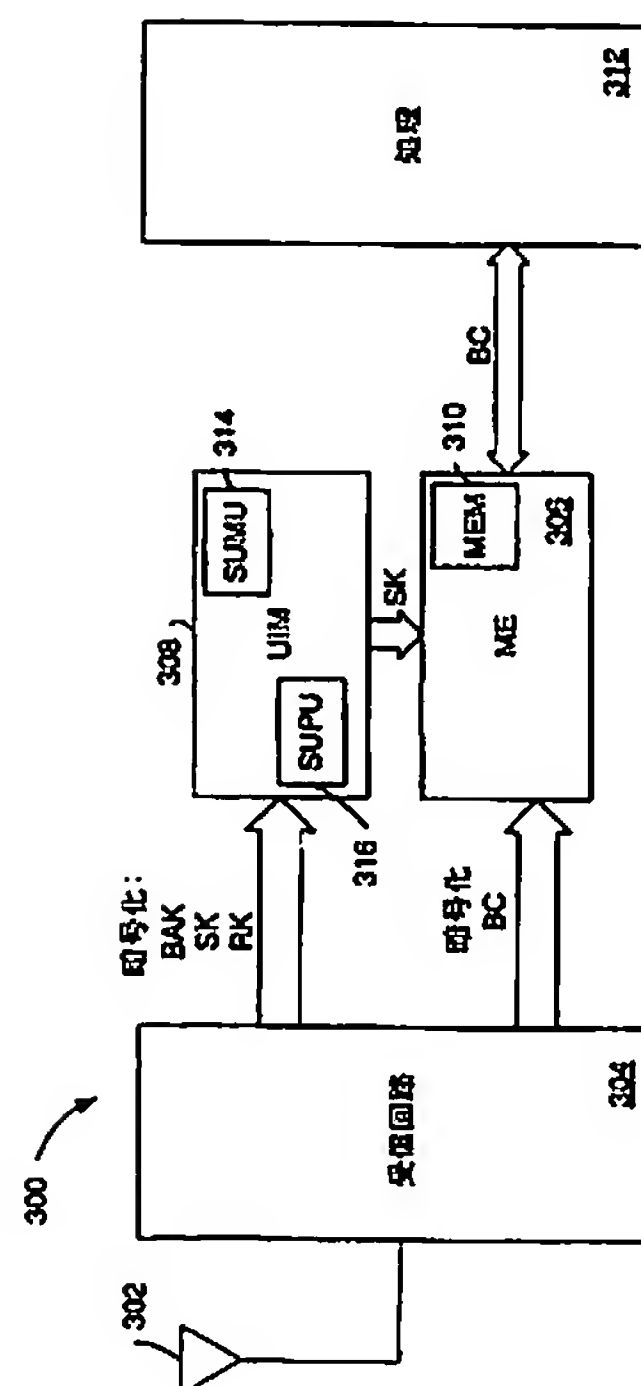
【圖 2】



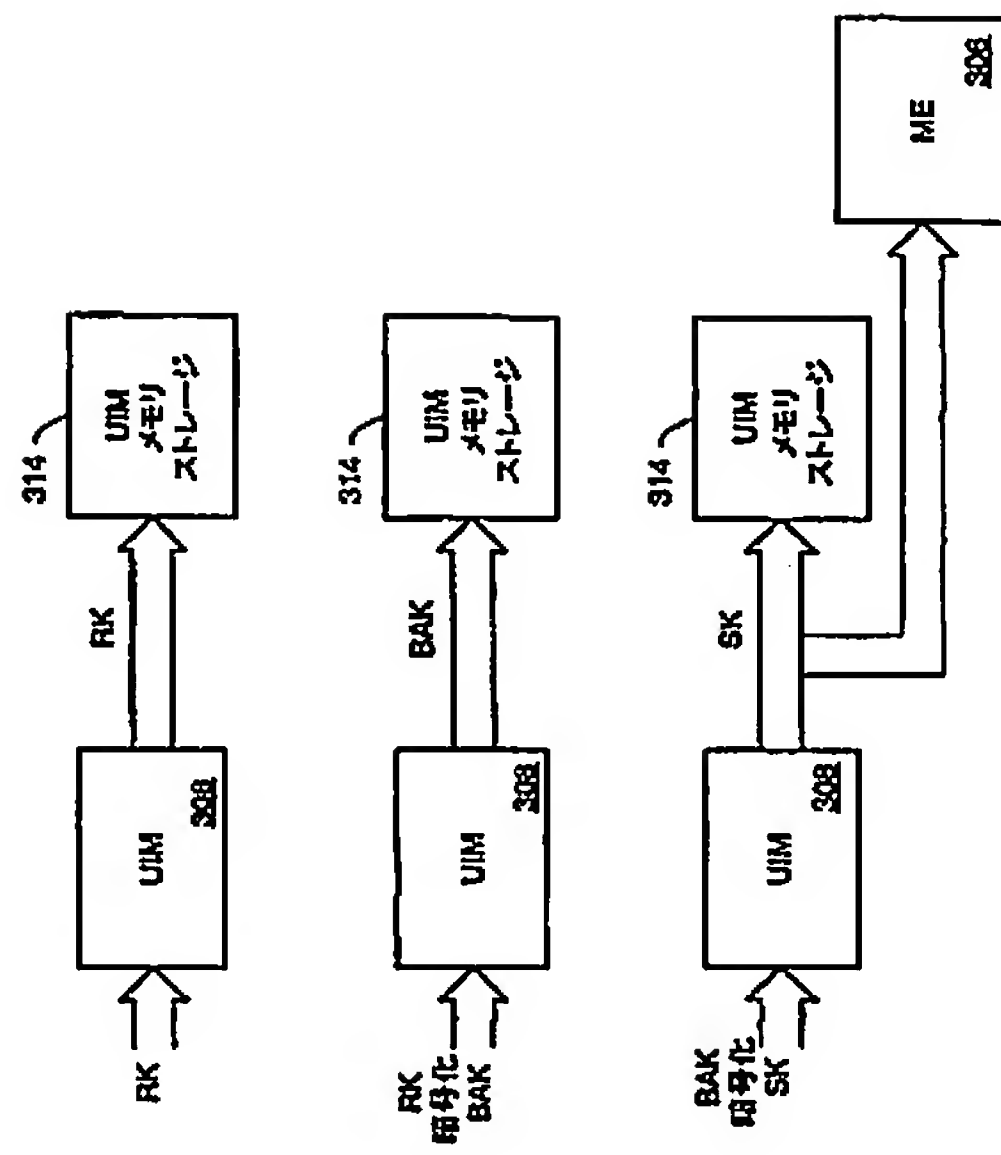
【図 3】



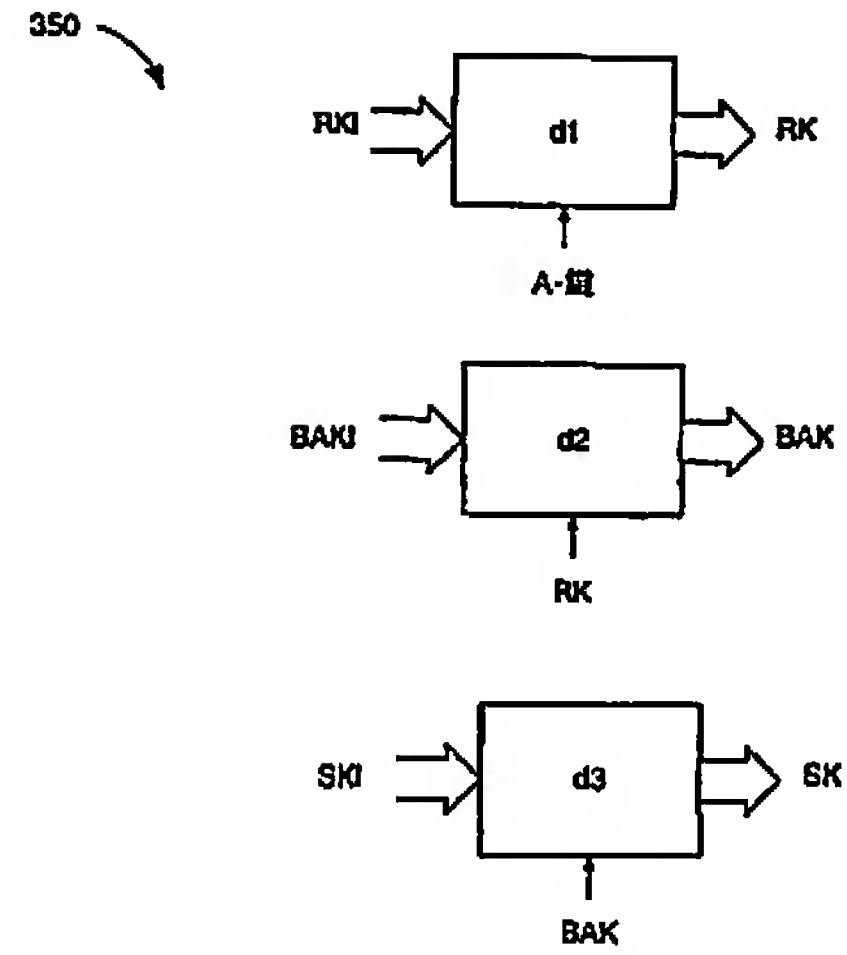
【 図 4 】



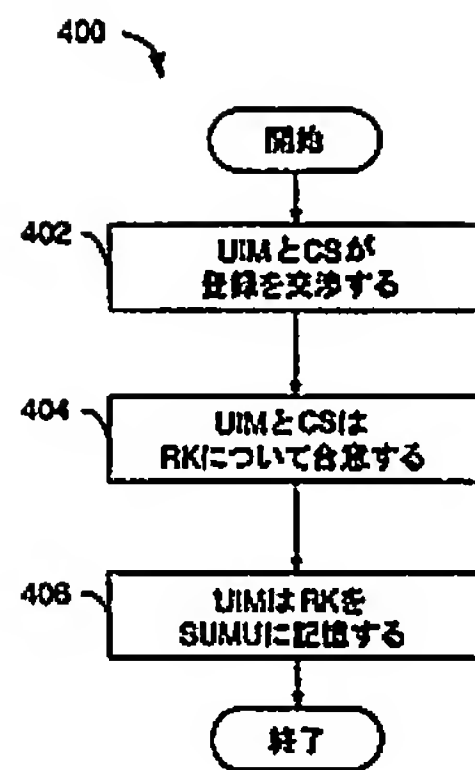
【図5】



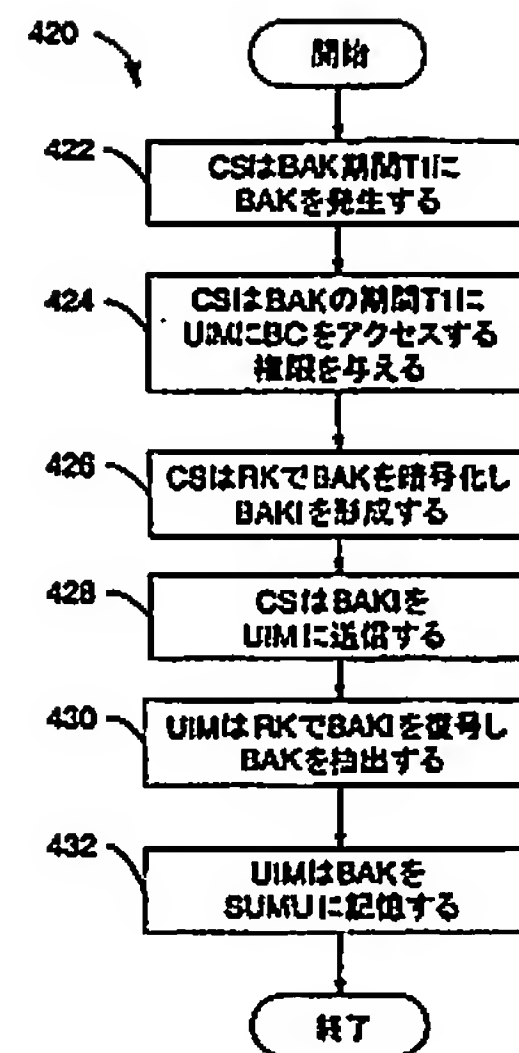
【図6】



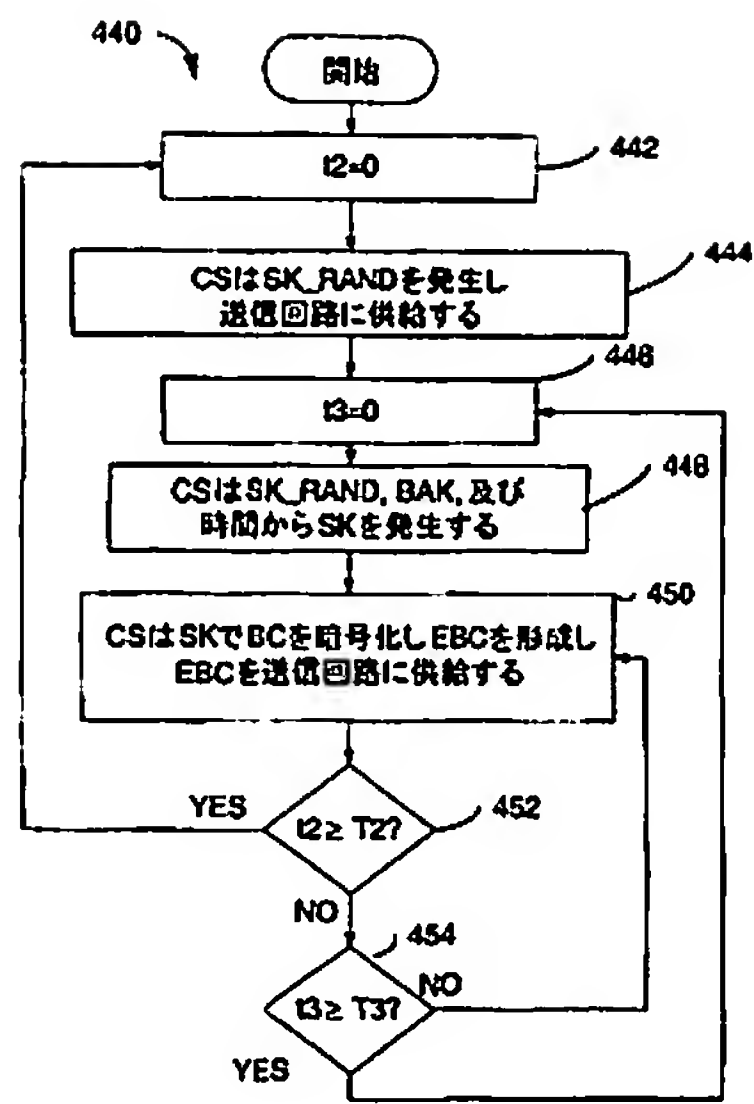
【図7A】



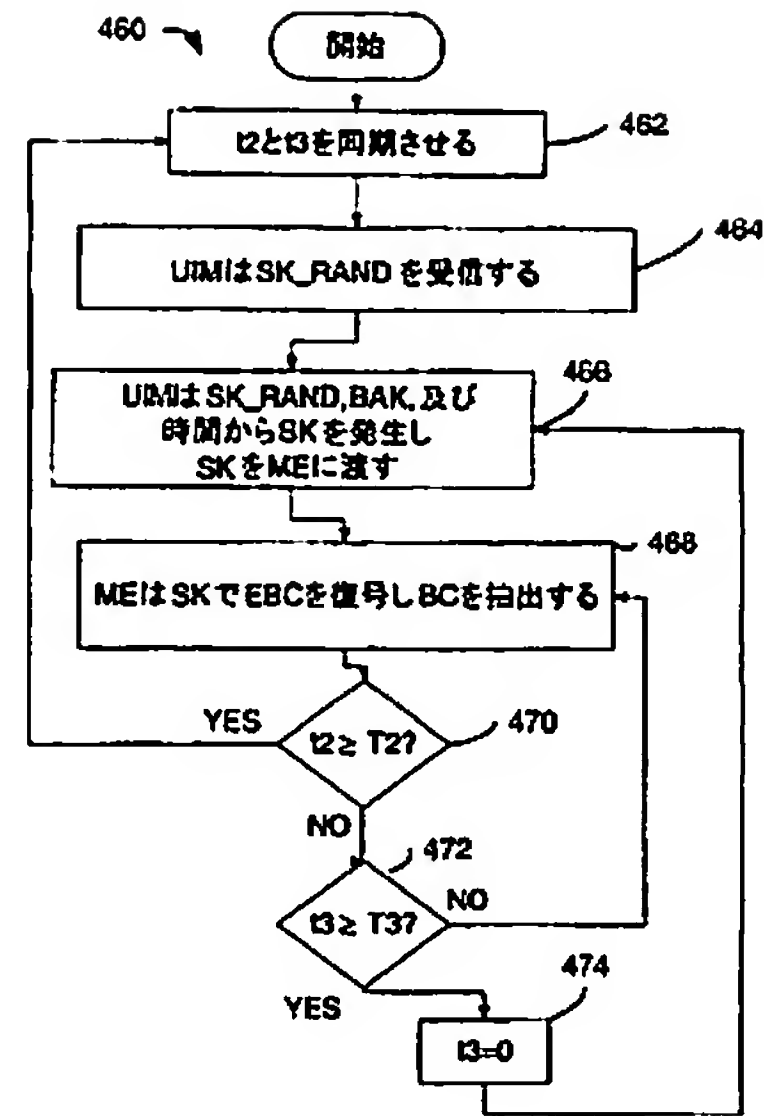
【図7B】



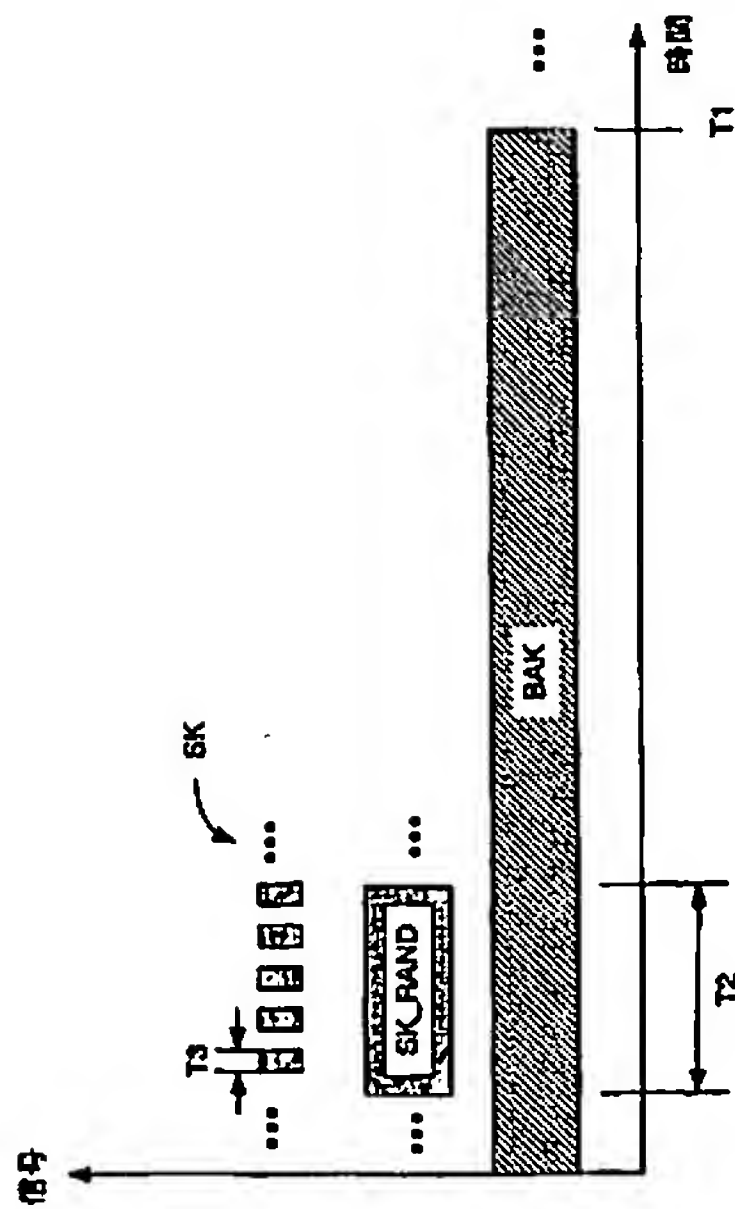
【図 7 C】



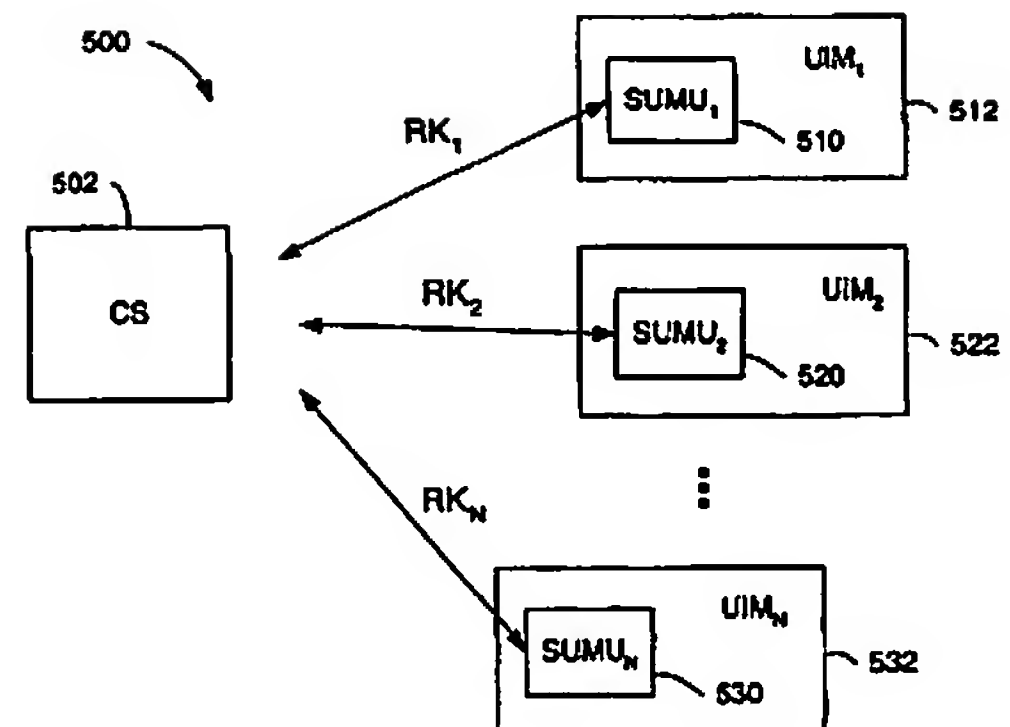
【図 7 D】



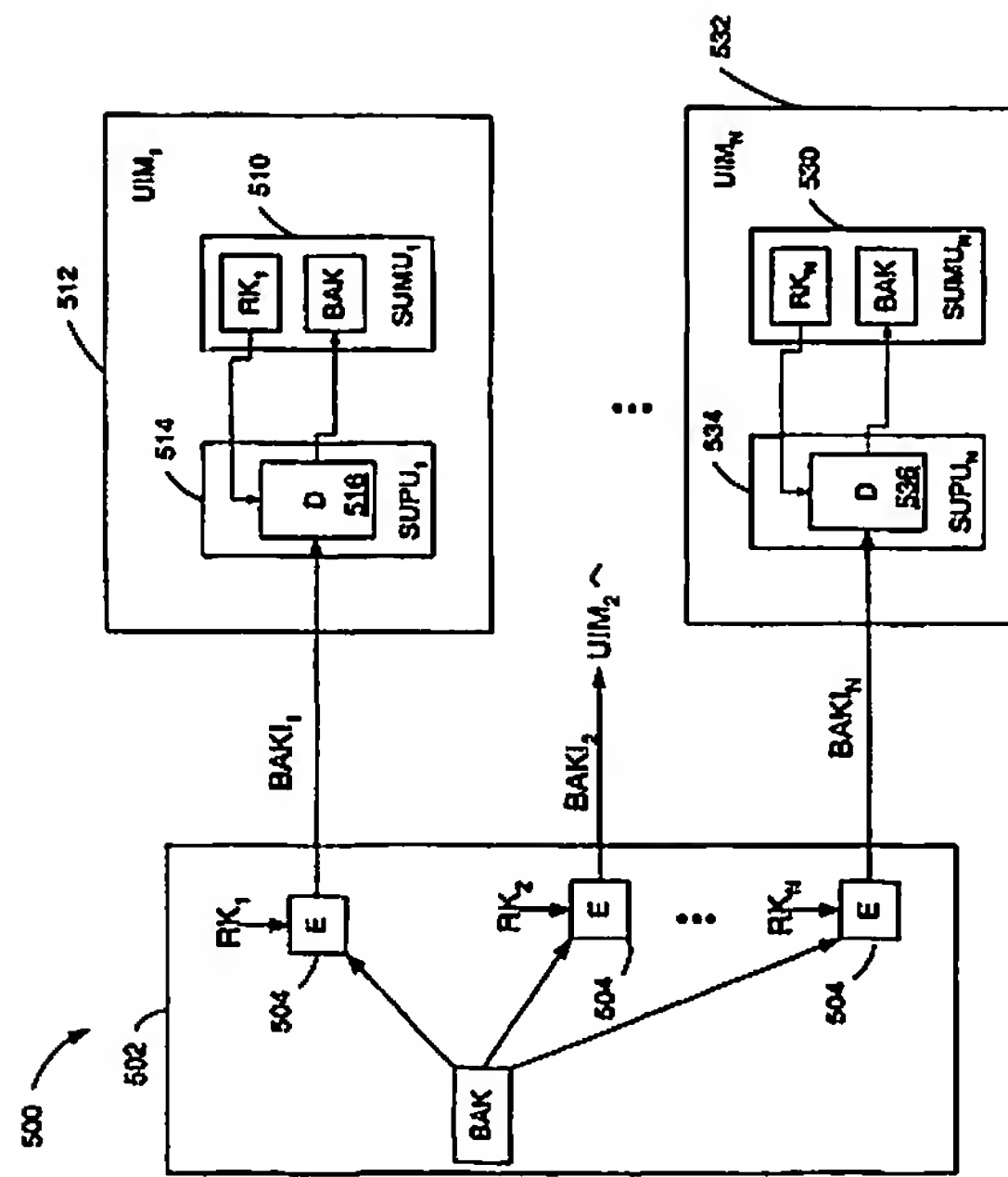
【図 7 E】



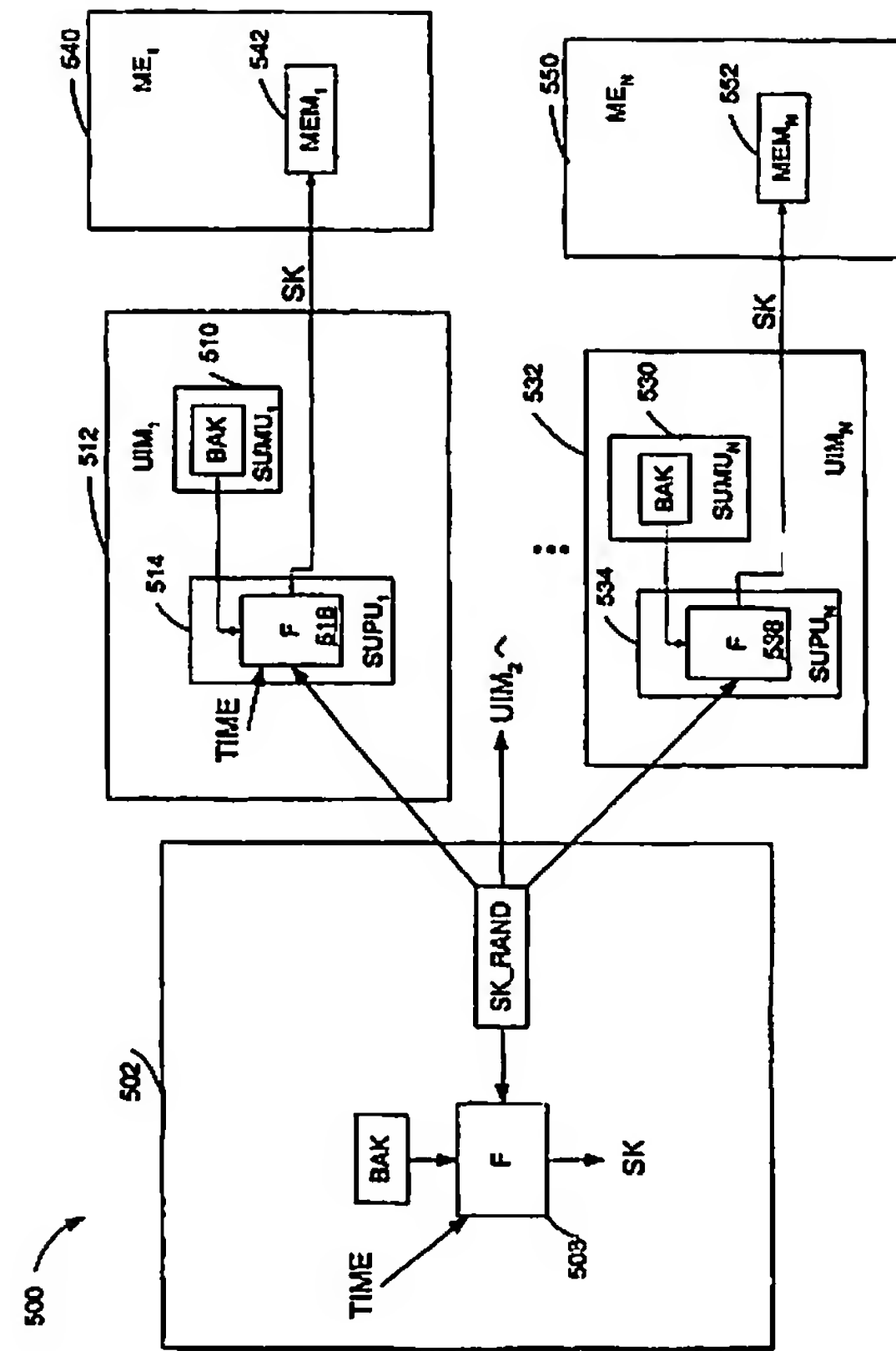
【図 8 A】



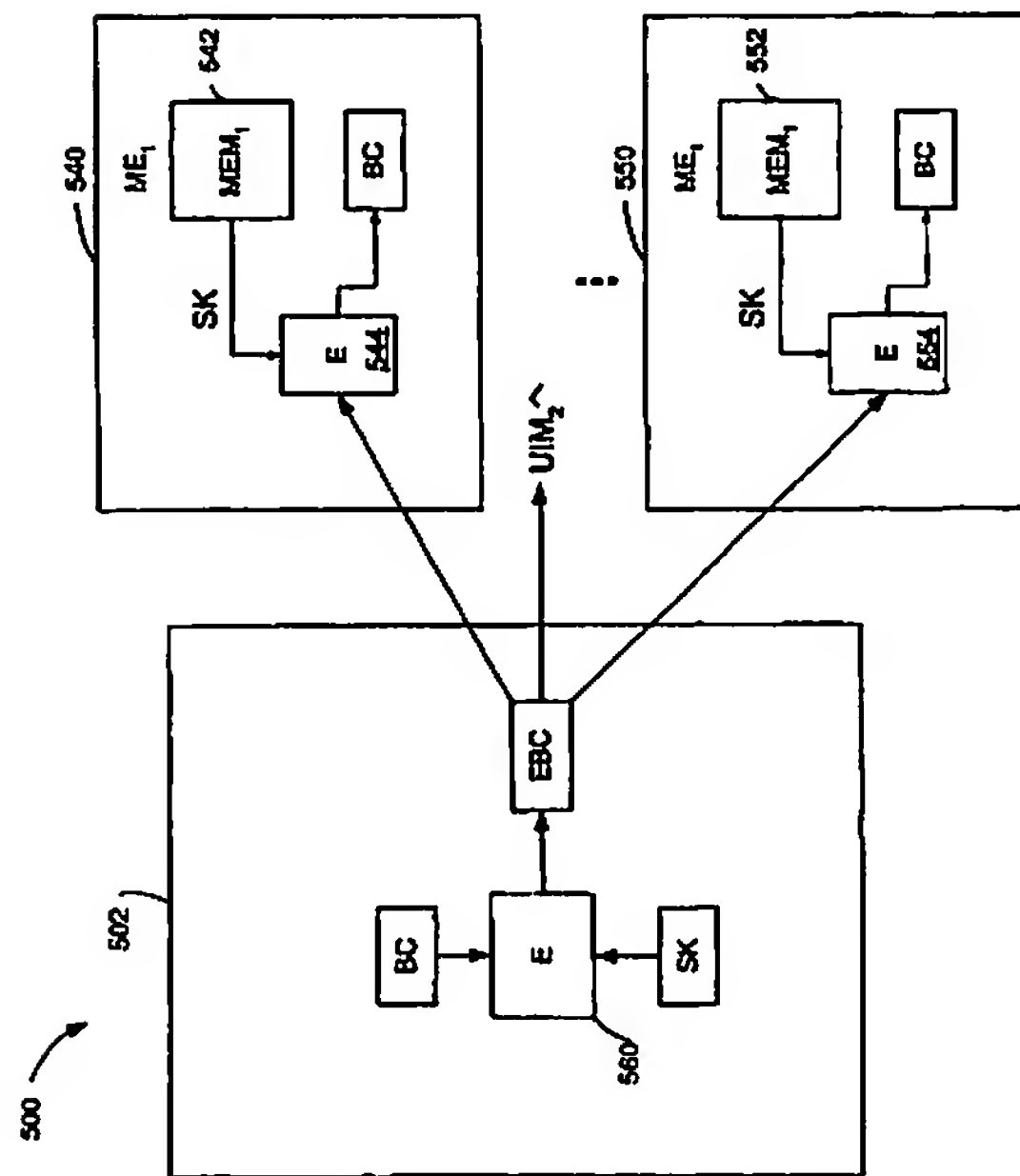
【図 8 B】



【図 8 C】



【図 8 D】



【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
10 October 2002 (10.10.2002)

PCT

(16) International Publication Number
WO 02/080449 A1(51) International Patent Classification:
H04L 9/00, H04Q 7/38

(74) Agents: WADSWORTH, Philip, R. et al.; Qualcomm Incorporated, 5775 La Jolla Village Drive, San Diego, CA 92121-1714 (US).

(21) International Application Number: PCT/US02/02215

(22) Designated States (national): All AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CO, CZ, DE, DK, DM, DO, EC, EE, ES, FI, FR, GB, GR, GU, HK, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LU, LV, MA, MD, MG, MK, MN, MW, MX, MY, NZ, OM, PA, PE, PG, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(23) International Filing Date: 28 March 2002 (28.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60279770 28 March 2001 (28.03.2001) US
09/933,972 20 August 2001 (20.08.2001) US

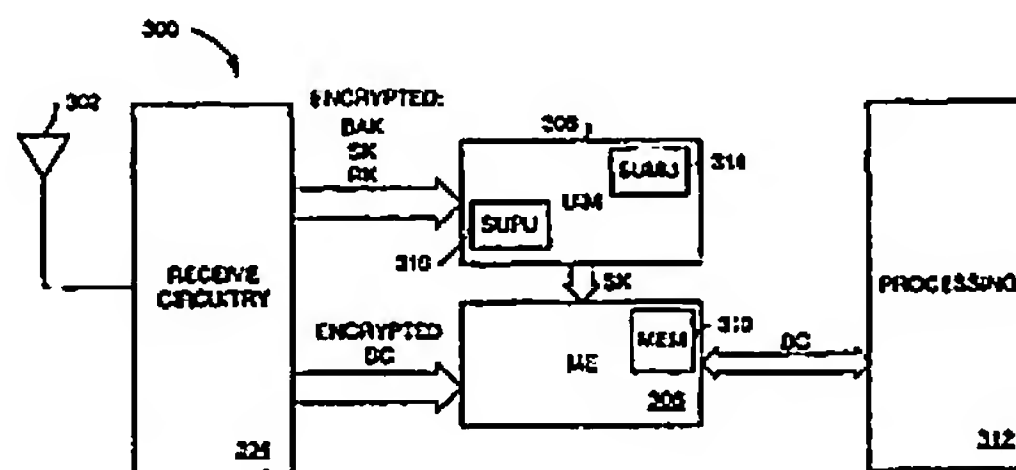
(84) Designated States (regional): ARIPO patent (GH, GM, LL, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GN, GQ, GW, ML, MR, NE, NG, TD, TG).

(71) Applicant: QUALCOMM INCORPORATED (USA); 5775 La Jolla Village Drive, San Diego, CA 92121-1714 (US).

(72) Inventors: HAYNES, Philip, 25-8 Deane Street, Darwood NSW 2134 (AU); ROSE, Gregory, G, 6 Kingston Avenue, Morinda, NSW 2137 (AU); REZAKHANI, Ramia, 10895 Chertina Avenue, San Diego, CA 92131 (US).

Published with international search report
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM



(57) Abstract: Method and apparatus for secure transmissions. Each user is provided a registration key. A long-time updated broadcast key is encrypted using the registration key and provided periodically to a user. A short-time updated key is encrypted using the broadcast key and provided periodically to a user. Broadcasts are then encrypted using the short-time key, wherein the user decrypts the broadcast message using the short-time key.

WO 02/080449 A1

**METHOD AND APPARATUS FOR SECURITY IN A DATA
PROCESSING SYSTEM**

BACKGROUND

Claim of Priority under 35 U.S.C. §120

[1001] The present Application for Patent claims priority of U.S. Provisional Application No. 60/279,970, filed March 28, 2001, assigned to the assignee hereof and hereby expressly incorporated by reference herein.

Reference to Co-Pending Applications for Patent

[1002] The present invention is related to the following Applications for Patent in the U.S. Patent & Trademark Office:

"METHOD AND APPARATUS FOR OVERHEAD MESSAGING IN A WIRELESS COMMUNICATION SYSTEM" by Nikolai Leung, having Attorney Docket No. 010439, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein;

"METHOD AND APPARATUS FOR OUT-OF-BAND TRANSMISSION OF BROADCAST SERVICE OPTION IN A WIRELESS COMMUNICATION SYSTEM" by Nikolai Leung, having Attorney Docket No. 010437, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein;

"METHOD AND APPARATUS FOR BROADCAST SIGNALING IN A WIRELESS COMMUNICATION SYSTEM" by Nikolai Leung, having Attorney Docket No. 010438, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein;

"METHOD AND APPARATUS FOR TRANSMISSION FRAMING IN A WIRELESS COMMUNICATION SYSTEM" by Raymond Hsu, having Attorney Docket No. 010498, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein;

"METHOD AND APPARATUS FOR DATA TRANSPORT IN A WIRELESS COMMUNICATION SYSTEM" by Raymond Hsu, having Attorney Docket No. 010499, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein; and

"METHOD AND APPARATUS FOR HEADER COMPRESSION IN A WIRELESS COMMUNICATION SYSTEM" by Raymond Hsu, having Attorney Docket No. 010500, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein.

Field

[1003] The present invention relates to data processing systems generally and specifically, to methods and apparatus for security in a data processing system.

Background

[1004] Security in data processing and information systems, including communications systems, contributes to accountability, fairness, accuracy, confidentiality, operability, as well as a plethora of other desired criteria. Encryption, or the general field of cryptography, is used in electronic commerce, wireless communications, broadcasting, and has an unlimited range of applications. In electronic commerce, encryption is used to prevent fraud in and verify financial transactions. In data processing systems, encryption is used to verify a participant's identity. Encryption is also used to prevent hacking, protect Web pages, and prevent access to confidential documents.

[1005] Asymmetric encryption system, often referred to as a cryptosystem, uses a same key (i.e., the secret key) to encrypt and decrypt a message. Whereas an asymmetric encryption system uses a first key (i.e., the public key) to encrypt a message and uses a different key (i.e., the private key) to decrypt it. Asymmetric cryptosystems are also called public key cryptosystems. A problem exists in symmetric cryptosystems in the secure provision of the secret key from a sender to a recipient. Further, a problem exists when keys or other encryption mechanisms are updated frequently. In a data processing system

WO 02/010449

PCT/US02/09335

3

methods of securely updating keys incur processing time, memory storage and other processing overhead. In a wireless communication system, updating keys uses valuable bandwidth used for transmission.

[1008] The prior art does not provide a method for updating keys to a large group of mobile stations in order that they may access an encrypted broadcast. There is a need, therefore, for a secure and efficient method of updating keys in a data processing system. Further, there is a need for a secure and efficient method of updating keys in a wireless communication system.

SUMMARY

[1007] Embodiments disclosed herein address the above stated needs by providing a method for security in a data processing system.

[1008] In one aspect a method for secure transmissions includes determining a registration key specific to a participant in a transmission, determining a first key, encrypting the first key with the registration key, determining a second key, encrypting the second key with the first key and updating the first and second keys.

[1009] In another aspect, a method for secure reception of a transmission includes receiving a registration key specific to a participant in a transmission, receiving a first key, decrypting the first key with the registration key, receiving a second key, decrypting the second key with the first key, receiving a broadcast stream of information, and decrypting the broadcast stream of information using the second key.

[1010] In still another aspect a wireless communication system supporting a broadcast service option has an infrastructure element including a receive circuitry, a user identification unit, operative to recover a short-time key for decrypting a broadcast message, and a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message. The user identification unit includes a processing unit operative to decrypt key information, and a memory storage unit for storing a registration key.

BRIEF DESCRIPTION OF THE DRAWINGS

- [1011] FIG. 1A is a diagram of a cryptosystem.
- [1012] FIG. 1B is a diagram of a symmetric cryptosystem.
- [1013] FIG. 1C is a diagram of an asymmetric cryptosystem.
- [1014] FIG. 1D is a diagram of a PGP encryption system.
- [1015] FIG. 1E is a diagram of a PGP decryption system.
- [1016] FIG. 2 is a diagram of a spread spectrum communication system that supports a number of users.
- [1017] FIG. 3 is a block diagram of the communication system supporting broadcast transmissions.
- [1018] FIG. 4 is a block diagram of a mobile station in a wireless communication system.
- [1019] FIG. 5 is a model describing the updating of keys within a mobile station used for controlling broadcast access.
- [1020] FIG. 6 is a model describing cryptographic operations within a UIM.
- [1021] FIGs. 7A-7D illustrate a method of implementing security encryption in a wireless communication system supporting broadcast transmissions.
- [1022] FIG. 7E is a timing diagram of key update periods of a security option in a wireless communication system supporting broadcast transmissions.
- [1023] FIGs. 8A-8D illustrate application of a security encryption method in a wireless communication system supporting broadcast transmissions.

DETAILED DESCRIPTION

[1024] The word "exemplary" is used exclusively herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[1025] Wireless communication systems are widely deployed to provide various types of communication such as voice, data, and so on. These systems may be based on code division multiple access (CDMA), time division multiple access (TDMA), or some other modulation techniques. A CDMA system

provides certain advantages over other types of system, including increased system capacity.

[1026] A system may be designed to support one or more standards such as the "TIA/EIA/IS-95-B Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System" referred to herein as the IS-95 standard, the standard offered by a consortium named "3rd Generation Partnership Project" referred to herein as 3GPP, and embodied in a set of documents including Document Nos. 3G TS 25.211, 3G TS 25.212, 3G TS 25.213, and 3G TS 25.214, 3G TS 25.302, referred to herein as the W-CDMA standard, the standard offered by a consortium named "3rd Generation Partnership Project 2" referred to herein as 3GPP2, and TR-45.5 referred to herein as the cdma2000 standard, formerly called IS-2000 MC. The standards cited hereinabove are hereby expressly incorporated herein by reference.

[1027] Each standard specifically defines the processing of data for transmission from base station to mobile, and vice versa. As an exemplary embodiment the following discussion considers a spread-spectrum communication system consistent with cdma2000 systems. Alternate embodiments may incorporate another standard/system. Still other embodiments may apply the security methods disclosed herein to any type of data processing system using a cryptosystem.

[1028] A cryptosystem is a method of disguising messages thus allowing a specific group of users to extract the message. FIG. 1A illustrates a basic cryptosystem 10. Cryptography is the art of creating and using cryptosystems. Cryptanalysis is the art of breaking cryptosystems, i.e., receiving and understanding the message when you are not within the specific group of users allowed access to the message. The original message is referred to as a plaintext message or plaintext. The encrypted message is called a ciphertext, wherein encryption includes any means to convert plaintext into ciphertext. Decryption includes any means to convert ciphertext into plaintext, i.e., recover the original message. As illustrated in FIG. 1A, the plaintext message is encrypted to form a ciphertext. The ciphertext is then received and decrypted to recover the plaintext. While the terms plaintext and ciphertext generally refer to data, the concepts of encryption may be applied to any digital information, including audio and video data presented in digital form. While the description

of the invention provided herein uses the term plaintext and ciphertext consistent with the art of cryptography, these terms do not exclude other forms of digital communications.

[1029] A cryptosystem is based on secrets. A group of entities shares a secret if an entity outside this group cannot obtain the secret without significantly large amount of resources. This secret is said to serve as a security association between the groups of entities.

[1030] A cryptosystem may be a collection of algorithms, wherein each algorithm is labeled and the labels are called keys. A symmetric encryption system, often referred to as a cryptosystem, uses a same key (i.e., the secret key) to encrypt and decrypt a message. A symmetric encryption system 20 is illustrated in FIG. 1B, wherein both the encryption and decryption utilize a same private key.

[1031] In contrast, an asymmetric encryption system uses a first key (i.e., the public key) to encrypt a message and uses a different key (i.e., the private key) to decrypt it. FIG. 1C illustrates an asymmetric encryption system 30 wherein one key is provided for encryption and a second key for decryption. Asymmetric cryptosystems are also called public key cryptosystems. The public key is published and available for encrypting any message, however, only the private key may be used to decrypt the message encrypted with the public key.

[1032] A problem exists in symmetric cryptosystems in the secure provision of the secret key from a sender to a recipient. In one solution a courier may be used to provide the information, or, a more efficient and reliable solution may be to use a public key cryptosystem, such as a public-key cryptosystem defined by Rivest, Shamir, and Adleman (RSA) which is discussed hereinbelow. The RSA system is used in the popular security tool referred to as Pretty Good Privacy (PGP), which is further detailed hereinbelow. For instance, an originally recorded cryptosystem altered letters in a plaintext by shifting each letter by n in the alphabet, wherein n is a predetermined constant integer value. In such a scheme, an "A" is replaced with a "D," etc., wherein a given encryption scheme may incorporate several different values of n . In this encryption scheme " n " is the key. Intended recipients are provided the encryption scheme prior to receipt of a ciphertext. In this way, only those knowing the key should be able to decrypt the ciphertext to recover the plaintext. However, by calculating the key

with knowledge of encryption, unintended parties may be able to intercept and decrypt the ciphertext, creating a security problem.

[1033] More complicated and sophisticated cryptosystems employ strategic keys that deter interception and decryption from unintended parties. A classic cryptosystem employs encryption functions E and decryption functions D such that:

$$D_K(E_K(P)) = P, \text{ for any plaintext } P. \quad (1)$$

[1034] In a public-key cryptosystem, E_K is easily computed from a known "public key" Y which in turn is computed from K . Y is published, so that anyone can encrypt messages. The decryption function D_K is computed from public key Y , but only with knowledge of a private key K . Without the private key K an unintended recipient may not decrypt the ciphertext so generated. In this way only the recipient who generated K can decrypt messages.

[1035] RSA is a public-key cryptosystem defined by Rivest, Shamir, and Adleman. As an example, consider plaintexts as positive integers up to 2^{12} . Keys are quadruples (p, q, e, d) , with p given as a 256-bit prime number, q as a 256-bit prime number, and d and e large numbers with $(de - 1)$ divisible by $(p-1)(q-1)$. Further, define the encryption function as:

$$E_K(P) = P^e \bmod pq, D_K(C) = C^d \bmod pq. \quad (2)$$

[1036] While, E_K is easily computed from the pair (pq, e) , there is no known simple way to compute D_K from the pair (pq, e) . Therefore, the recipient that generates K can publish (pq, e) . It is possible to send a secret message to the recipient, as he is the one able to read the message.

[1037] PGP combines features from symmetric and asymmetric encryption. FIGs. 1D and 1E illustrate a PGP cryptosystem 50, wherein a plaintext message is encrypted and recovered. In FIG. 1D, the plaintext message is compressed to save modem transmission time and disk space. Compression strengthens cryptographic security by adding another level of translation to the encrypting and decrypting processing. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby enhancing resistance to cryptanalysis. Note that one embodiment does not compress plaintext or other messages that are too short to compress or which don't compress well aren't compressed.

[1038] PGP then creates a *session key*, which is a one-time-only secret key. This key is a random number that may be generated from any random event(s), such as random movements of mouse and the keystrokes while typing. The session key works with a secure encryption algorithm to encrypt the plaintext, resulting in ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

[1039] For decryption, as illustrated in FIG. 1E, the recipient's copy of PGP uses a private key to recover the temporary session key, which PGP then uses to decrypt the conventionally encrypted ciphertext. The combination of encryption methods takes advantage of the convenience of public key encryption and the speed of symmetric encryption. Symmetric encryption is generally much faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. In combination, performance and key distribution are improved without any sacrifice in security.

[1040] A key is a value that works with a cryptographic algorithm to produce a specific ciphertext. Keys are basically very large numbers. Key size is measured in bits. In public key cryptography, security increases with key size, however, public key size and the symmetric encryption private key size are not generally related. While the public and private keys are mathematically related, a difficulty arises in deriving a private key given only a public key. Deriving the private key is possible given enough time and computing power, making the selection of key size an important security issue. The goal is to have a large key that is secure, while maintaining key size sufficiently small for quick processing. An additional consideration is the expected interceptor, specifically, what is the importance of a message to a third party, and how much resource does a third party have to decrypt.

[1041] Larger keys will be cryptographically secure for a longer period of time. Keys are stored in encrypted form. PGP specifically stores keys in two files; one for public keys and one for private keys. These files are called *keyrings*. In application, a PGP encryption system adds the public keys of target recipients to the sender's public keyring. The sender's private keys are stored on the sender's private keyring.

[1042] As discussed in the examples given hereinabove, the method of distributing the keys used for encryption and decryption can be complicated. The "key exchange problem" involves first ensuring that keys are exchanged such that both the sender and receiver can perform encryption and decryption, respectively, and for bi-directional communication, such that the sender and receiver can both encrypt and decrypt messages. Further, it is desired that key exchange be performed so as to preclude interception by a third unintended party. Finally, an additional consideration is authentication providing assurance to the receiver that a message was encrypted by an intended sender and not a third party. In a private key exchange system, the keys are exchanged secretly providing improved security upon successful key exchange and valid authentication. Note that the private key encryption scheme implicitly provides authentication. The underlying assumption in a private key cryptosystem is that only the intended sender will have the key capable of encrypting messages delivered to the intended receiver. While public-key cryptographic methods solve a critical aspect of the 'key-exchange problem', specifically their resistance to analysis even with the presence a passive eavesdropper during exchange of keys, they do not solve all problems associated with key exchange. In particular, since the keys are considered 'public knowledge,' (particularly with RSA) some other mechanism is desired to provide authentication, as possession of keys alone (sufficient to encrypt messages) is no evidence of a particular unique identity of the sender, nor is possession of a corresponding decryption key by itself enough to establish the identity of the recipient.

[1043] One solution is to develop a key distribution mechanism that assures that listed keys are actually those of the given entities, sometimes called a trusted authority, certificate authority, or third party escrow agent. The authority typically does not actually generate keys, but does ensure that the lists of keys and associated identities kept and advertised for reference by senders and receivers are correct and uncompromised. Another method relies on users to distribute and track each other's keys and trust in an informal, distributed fashion. Under RSA, if a user wishes to send evidence of their identity in addition to an encrypted message, a signature is encrypted with the private key. The receiver can use the RSA algorithm in reverse to verify that the information decrypts, such that only the sender could have encrypted the plaintext by use of

the secret key. Typically the encrypted 'signature' is a 'message digest' that comprises a unique mathematical 'summary' of the secret message (if the signature were static across multiple messages, once known previous receivers could use it falsely). In this way, theoretically only the sender of the message could generate a valid signature for that message, thereby authenticating it for the receiver.

[1044] A message digest is often computed using a cryptographic hash function. A cryptographic hash function computes a value (with a fixed number of bits) from any input, regardless of the length of the input. One property of a cryptographic hash function is this: given an output value, it is computationally difficult to determine an input that will result in that output. An example of a cryptographic hash function is SHA-1 as described in "Secure Hash Standard," FIPS PUB 180-1, promulgated by the Federal Information Processing Standards Publications (FIPS PUBS) and issued by the National Institute of Standards and Technology.

[1045] FIG. 2 serves as an example of a communications system 100 that supports a number of users and is capable of implementing at least some aspects and embodiments of the invention. Any of a variety of algorithms and methods may be used to schedule transmissions in system 100. System 100 provides communication for a number of cells 102A through 102G, each of which is serviced by a corresponding base station 104A through 104G, respectively. In the exemplary embodiment, some of base stations 104 have multiple receive antennas and others have only one receive antenna. Similarly, some of base stations 104 have multiple transmit antennas, and others have single transmit antennas. There are no restrictions on the combinations of transmit antennas and receive antennas. Therefore, it is possible for a base station 104 to have multiple transmit antennas and a single receive antenna, or to have multiple receive antennas and a single transmit antenna, or to have both single or multiple transmit and receive antennas.

[1046] Terminals 106 in the coverage area may be fixed (i.e., stationary) or mobile. As shown in FIG. 2, various terminals 106 are dispersed throughout the system. Each terminal 106 communicates with at least one and possibly more base stations 104 on the downlink and uplink at any given moment depending on, for example, whether soft handoff is employed or whether the

terminal is designed and operated to (concurrently or sequentially) receive multiple transmissions from multiple base stations. Soft handoff in CDMA communications systems is well known in the art and is described in detail in U.S. Patent No. 5,101,501, entitled "METHOD AND SYSTEM FOR PROVIDING A SOFT HANDOFF IN A CDMA CELLULAR TELEPHONE SYSTEM," which is assigned to the assignee of the present invention.

[1047] The downlink refers to transmission from the base station to the terminal, and the uplink refers to transmission from the terminal to the base station. In the exemplary embodiment, some of terminals 108 have multiple receive antennas and others have only one receive antenna. In FIG. 2, base station 104A transmits data to terminals 106A and 106J on the downlink, base station 104B transmits data to terminals 106B and 106J, base station 104C transmits data to terminal 106C, and so on.

[1048] Increasing demand for wireless data transmission and the expansion of services available via wireless communication technology have led to the development of specific data services. One such service is referred to as High Data Rate (HDR). An exemplary HDR service is proposed in "EIA/TIA-15856 cdma2000 High Rate Packet Data Air Interface Specification" referred to as "the HDR specification." HDR service is generally an overlay to a voice communication system that provides an efficient method of transmitting packets of data in a wireless communication system. As the amount of data transmitted and the number of transmissions increases, the limited bandwidth available for radio transmissions becomes a critical resource. There is a need, therefore, for an efficient and fair method of scheduling transmissions in a communication system that optimizes use of available bandwidth. In the exemplary embodiment, system 100 illustrated in FIG. 2 is consistent with a CDMA type system having HDR service.

[1049] According to one embodiment, the system 100 supports a high-speed multimedia broadcasting service referred to as High-Speed Broadcast Service (HSBS). An example application for HSBS is video streaming of movies, sports events, etc. The HSBS service is a packet data service based on the Internet Protocol (IP). According to the exemplary embodiment, a service provider indicates the availability of such high-speed broadcast service to the users. The users desiring the HSBS service subscribe to receive the service and may

discover the broadcast service schedule through advertisements, Short Message System (SMS), Wireless Application Protocol (WAP), etc. Mobile users are referred to as Mobile Stations (MSs). Base Stations (BSs) transmit HSBS related parameters in overhead messages. When an MS desires to receive the broadcast session, the MS reads the overhead messages and learns the appropriate configurations. The MS then tunes to the frequency containing the HSBS channel, and receives the broadcast service content.

[1050] The service being considered is a high-speed multimedia broadcasting service. This service is referred to as High-Speed Broadcast Service (HSBS) in this document. One such example is video streaming of movies, sports events, etc. This service will likely be a packet data service based on the Internet Protocol (IP).

[1051] The service provider will indicate the availability of such high-speed broadcast service to the users. The mobile station users who desire such service will subscribe to receive this service and may discover the broadcast service schedule through advertisements, SMS, WAP, etc. Base stations will transmit broadcast service related parameters in overhead messages. The mobiles that wish to listen to the broadcast session will read these messages to determine the appropriate configurations, tune to the frequency containing the high-speed broadcast channel, and start receiving the broadcast service content.

[1052] There are several possible subscription/revenue models for HSBS service, including free access, controlled access, and partially controlled access. For free access, no subscription is needed by the mobiles to receive the service. The BS broadcasts the content without encryption and interested mobiles can receive the content. The revenue for the service provider can be generated through advertisements that may also be transmitted in the broadcast channel. For example, upcoming movie-clips can be transmitted for which the studios will pay the service provider.

[1053] For controlled access, the MS users subscribe to the service and pay the corresponding fee to receive the broadcast service. Unsubscribed users are not able to receive the HSBS service. Controlled access can be achieved by encrypting the HSBS transmission/content so that only the subscribed users can decrypt the content. This may use over-the-air encryption key exchange

procedures. This scheme provides strong security and prevents theft-of-service.

[1054] A hybrid access scheme, referred to as partial controlled access, provides the HSBS service as a subscription-based service that is encrypted with intermittent unencrypted advertisement transmissions. Those advertisements may be intended to encourage subscriptions to the encrypted HSBS service. Schedule of these unencrypted segments could be known to the MS through external means.

[1055] A wireless communication system 200 is illustrated in FIG. 3, wherein video and audio information is provided to Packetized Data Service Network (PDSN) 202 by a Content Server (CS) 201. The video and audio information may be from televised programming or a radio transmission. The information is provided as packetized data, such as in IP packets. The PDSN 202 processes the IP packets for distribution within an Access Network (AN). As illustrated the AN is defined as the portions of the system including a BS 204 in communication with multiple MS 206. The PDSN 202 is coupled to the BS 204. For HSBS service, the BS 204 receives the stream of information from the PDSN 202 and provides the information on a designated channel to subscribers within the system 200. To control the access, the content is encrypted by the CS 201 before being provided to the PDSN 202. The subscribed users are provided with the decryption key so that the IP packets can be decrypted.

[1056] FIG. 4 details an MS 300, similar to MS 206 of FIG. 3. The MS 300 has an antenna 302 coupled to receive circuitry 304. The MS 300 receives transmissions from a BS (not shown) similar to BS 204 of FIG. 3. The MS 300 includes a User Identification Module (UIM) 308 and a Mobile Equipment (ME) 306. The receive circuitry is coupled to the UIM 308 and the ME 306. The UIM 308 applies verification procedures for security of the HSBS transmission and provides various keys to the ME 306. The ME 306 may be coupled to processing unit 312. The ME 306 performs substantial processing, including, but not limited to, decryption of HSBS content streams. The ME 306 includes a memory storage unit, MEM 310. In the exemplary embodiment the data in the ME 306 processing (not shown) and the data in the ME memory storage unit, MEM 310 may be accessed easily by a non-subscriber by the use of limited resources, and therefore, the ME 306 is said to be insecure. Any information

passed to the ME 306 or processed by the ME 308 remains securely secret for only a short amount of time. It is therefore desired that any secret information, such as key(s), shared with the ME 308 be changed often.

[1057] The UIM 308 is trusted to store and process secret information (such as encryption keys) that should remain secret for a long time. As the UIM 308 is a secure unit, the secrets stored therein do not necessarily require the system to change the secret information often. The UIM 308 includes a processing unit referred to as a Secure UIM Processing Unit (SUPU) 316 and memory storage unit referred to as a Secure UIM Memory Unit (SUMU) 314 that is trusted to be secure. Within the UIM 308, SUMU 314 stores secret information in such a way that as to discourage unauthorized access to the information. If the secret information is obtained from the UIM 308, the access will require a significantly large amount of resources. Also within the UIM 308, the SUPU 316 performs computations on values that may be external to the UIM 308 and/or internal to the UIM 308. The results of the computation may be stored in the SUMU 314 or passed to the ME 306. The computations performed with the SUPU 316 can only be obtained from the UIM 308 by an entity with significantly large amount of resources. Similarly, outputs from the SUPU 316 that are designated to be stored within the SUMU 314 (but not output to the ME 306) are designed such that unauthorized interception requires significantly large amount of resources. In one embodiment, the UIM 308 is a stationary unit within the MS 300. Note that in addition to the secure memory and processing within the UIM 308, the UIM 308 may also include non-secure memory and processing (not shown) for storing information including telephone numbers, e-mail address information, web page or URL address information, and/or scheduling functions, etc.

[1058] Alternate embodiments may provide a removable and/or reprogrammable UIM. In the exemplary embodiment, the SUPU 316 does not have significant processing power for functions beyond security and key procedures, such as to allow encryption of the broadcast content of the HSBS. Alternate embodiments may implement a UIM having stronger processing power.

[1059] The UIM is associated with a particular user and is used primarily to verify that the MS 300 is entitled to the privileges afforded the user, such as access to the mobile phone network. Therefore, a user is associated with the

UIM 308 rather than an MS 300. The same user may be associated with multiple UIM 308.

[1060] The broadcast service faces a problem in determining how to distribute keys to subscribed users. To decrypt the broadcast content at a particular time, the ME must know the current decryption key. To avoid theft-of-service, the decryption key should be changed frequently, for example, every minute. These decryption keys are called Short-term Keys (SK). The SK is used to decrypt the broadcast content for a short-amount of time so the SK can be assumed to have some amount of intrinsic monetary value for a user. For example, this intrinsic monetary value may be a portion of the registration costs. Assume that the cost of a non-subscriber obtaining SK from the memory storage unit, MEM 310, of a subscriber exceeds the intrinsic monetary value of SK. That is, the cost of obtaining SK (illegitimately) exceeds the reward, so there is no benefit. Consequently, there is no need to protect SK in the memory storage unit, MEM 310. However, if a secret key has a lifetime longer than that of an SK, then the cost of obtaining this secret key (illegitimately) is less than the reward. In this situation, there is a benefit in obtaining such a key from the memory storage unit, MEM 310. Hence, ideally the memory storage unit, MEM 310 will not store secrets with a lifetime longer than that of an SK.

[1061] The channels used by the CS (not shown) to distribute the SK to the various subscriber units are considered insecure. Therefore, when distributing a given SK, the CS desires to use a technique that hides the value of the SK from non-subscribed users. Furthermore, the CS distributes the SK to each of a potentially large number of subscribers for processing in respective MEs within a relatively short timeframe. Known secure methods of key transmission are slow and require transmission of a large number of keys, and are generally not feasible for the desired criteria. The exemplary embodiment is a feasible method of distributing decryption keys to a large set of subscribers within a small time-frame in such a way that non-subscribers cannot obtain the decryption keys.

[1062] In the exemplary embodiment, the MS 300 supports HSBS in a wireless communication system. To obtain access to HSBS, the user must register and then subscribe to the service. Once the subscription is enabled, the various keys are updated periodically. In the registration process the CS

and UIM 308 agree on a Registration Key (RK) that serves as a security association between the user and the CS. The CS may then send the UIM further secret information encrypted with the RK. The RK is kept as a secret in the UIM 308, and is unique to a given UIM, i.e., each user is assigned a different RK. The registration process alone does not give the user access to HSBS. As stated hereinabove, after registration the user subscribes to the service. In the subscription process the CS sends the UIM 308 the value of a common Broadcast Access Key (BAK). The CS sends the MS 300, and specifically UIM 308, the value of BAK encrypted using the RK unique to UIM 308. The UIM 308 is able to recover the value of the original BAK from the encrypted version using the RK. The BAK serves as a security association between the CS and the group of subscribed users. The CS then broadcasts data called SK Information (SKI) that is combined with the BAK in the UIM 308 to derive SK. The UIM 308 then passes SK to the ME 306. In this way, the CS can efficiently distribute new values of SK to the ME of subscribed users.

[1063] The following paragraphs discuss the registration process in more detail. When a user registers with a given CS, the UIM 308 and the CS (not shown) set-up a security association. That is, the UIM 308 and the CS agree on a secret key RK. The RK is unique to each UIM 308, although if a user has multiple UIMs then these UIMs may share the same RK dependent on the policies of the CS. This registration may occur when the user subscribes to a broadcast channel offered by the CS or may occur prior to subscription. A single CS may offer multiple broadcast channels. The CS may choose to associate the user with the same RK for all channels or require the user to register for each channel and associate the same user with different RKs on different channels. Multiple CSs may choose to use the same registration keys or require the user to register and obtain a different RK for each CS.

[1064] Two common scenarios for setting up this security association include the Authenticated Key Agreement (AKA) method (as used in 3GPP) and the Internet Key Exchange (IKE) method as used in IPsec. In either case the UIM memory unit SUMU 314 contains a secret key referred to as the A-key. As an example, the AKA method is described. In the AKA method the A-key is a secret known only to the UIM and a trusted third party (TTP): the TTP may consist of more than one entity. The TTP is typically the mobile service provider

with whom the user is registered. All communication between the CS and TTP is secure, and the CS trusts that the TTP will not assist unauthorized access to the broadcast service. When the user registers, the CS informs the TTP that the user wishes to register for the service and provides verification of the user's request. The TTP uses a function (similar to a cryptographic hash function) to compute the RK from the A-key and additional data called Registration Key Information (RKI). The TTP passes RK, RKI to the CS over a secure channel along with other data not relevant to this submission. The CS sends RKI to the MS 300. The receiver circuitry 304 passes RKI to the UIM 308 and possibly passes RKI to the ME 306. The UIM 308 computes RK from RKI and the A-key that is stored in the UIM memory unit SUMU 314. The RK is stored in the UIM memory unit SUMU 314 and is not provided directly to the ME 306. Alternate embodiments may use an IKE scenario or some other method to establish the RK. The RK serves as the security association between the CS and UIM 308.

[1085] In the AKA method, the RK is a secret shared between the CS, UIM and TTP. Therefore, as used herein, the AKA method implies that any security association between the CS and UIM implicitly includes the TTP. The inclusion of the TTP in any security association is not considered a breach of security, as the CS trusts the TTP not to assist in unauthorized access to the broadcast channel. As stated hereinabove, if a key is shared with the ME 306, it is desirable to change that key often. This is due to the risk of a non-subscriber accessing information stored in memory storage unit, MEM 310 and thus allowing access to a controlled or partially controlled service. The ME 306 stores SK (key information used for decrypting broadcast content) in memory storage unit, MEM 310. The CS must send sufficient information for subscribed users to compute SK. If the ME 306 of a subscribed user could compute SK from this information, then additional information required to compute SK cannot be secret. In this case, assume that the ME 306 of a non-subscribed user could also compute SK from this information. Hence, the value of SK must be computed in the SUPU 316, using a secret key shared by the CS and SUMU 314. The CS and SUMU 314 share the value of RK, however each user has a unique value of RK. There is insufficient time for the CS to encrypt SK with every value of RK and transmit these encrypted values to each subscribed user. Some other technique is required.

[1066] The following paragraphs discuss the subscription process in more detail. To ensure the efficient distribution of the security information SK, the CS periodically distributes a common Broadcast Access Key (BAK) to each subscriber UIM 308. For each subscriber the CS encrypts BAK using the corresponding RK to obtain a value called BAKI (BAK Information). The CS sends the corresponding BAKI to MS 300 of the subscribed user. For example, BAK may be transmitted as an IP packet encrypted using the RK corresponding to each MS. In the exemplary embodiment, the BAKI is an IPSec packet. In the exemplary embodiment, BAKI is an IPSec packet containing BAK that is encrypted using RK as the key. Since RK is a per-user key, the CS must send the BAK to each subscriber individually; thus, the BAK is not sent over the broadcast channel. The MS 300 passes the BAKI to the UIM 308. The SUPU 316 computes BAK using the value of RK stored in SUMU 314 and the value of BAKI. The value of BAK is then stored in the SUMU. In the exemplary embodiment, the BAKI contains a Security Parameter Index (SPI) value instructing the MS 300 to pass BAKI to the UIM 308, and instructing the UIM 308 to use the RK for decrypting the BAKI.

[1067] The period for updating the BAK is desired to be sufficient to allow the CS to send the BAK to each subscriber individually, without incurring significant overhead. Since the ME 306 is not trusted to keep secrets for a long time, the UIM 308 does not provide the BAK to the ME 306. The BAK serves as the security association between the CS and the group of subscribers of HSBS service.

[1068] The following paragraph discusses how the SK is updated following a successful subscription process. Within each period for updating the BAK, a short-term interval is provided during which SK is distributed on a broadcast channel. The CS uses a cryptographic function to determine two values SK and SKI (SK Information) such that SK can be determined from BAK and SKI. For example, SKI may be the encryption of SK using BAK as the key. In the exemplary embodiment, SKI is an IPSec packet containing SK that is encrypted using BAK as the key. Alternatively, SK may be the result of applying a cryptographic hash function to the concatenation of the blocks SKI and BAK.

[1069] Some portion of SKI may be predictable. For example, a portion of SKI may be derived from the system time during which this SKI is valid. This

portion, denoted SKI_A, need not be transmitted to the MS 300 as part of the broadcast service. The remainder of SKI, SKI_B may be unpredictable. The SKI_B need not be transmitted to the MS 300 as part of the broadcast service. The MS 300 reconstructs SKI from SKI_A and SKI_B and provides SKI to UIM 308. The SKI may be reconstructed within the UIM 308. The value of SKI must change for each new SK. Thus, either SKI_A and/or SKI_B must change when computing a new SK. The CS sends SKI_B to BS for broadcast transmission. The BS broadcasts SKI_B, which is detected by the antenna 302 and passed to the receive circuitry 304. Receive circuitry 304 provides SKI_B to the MS 300, wherein the MS 300 reconstructs SKI. The MS 300 provides SKI to UIM 308, wherein the UIM 308 obtains the SK using the BAK stored in SUMU 314. The SK is then provided by UIM 308 to ME 306. The ME 306 stores the SK in memory storage unit, MEM 310. The ME 306 uses the SK to decrypt broadcast transmissions received from the CS.

[1070] In the exemplary embodiment, the SKI also contains a Security Parameter Index (SPI) value instructing the MS 300 to pass SKI to the UIM 308, and instructing the UIM 308 to use the BAK for decrypting the SKI. After decryption, the UIM 308 passes the SK to the ME 306, wherein ME 306 uses the SK to decrypt broadcast content.

[1071] The CS and BS agree on some criteria for when SKI_B is to be transmitted. The CS may desire to reduce the intrinsic monetary value in each SK by changing SK frequently. In this situation, the desire to change SKI_B data is balanced against optimizing available bandwidth. The SKI_B may be transmitted on a channel other than the broadcast channel. When a user "tunes" to the broadcast channel, the receive circuitry 304 obtains information for locating the broadcast channel from a "control channel." It may be desirable to allow quick access when a user "tunes" to the broadcast channel. This requires the ME 306 to obtain SKI within a short amount of time. The ME 306 will already know SKI_A, however, the BS must provide SKI_B to ME 300 within this short amount of time. For example, the BS may frequently transmit SKI_B on the control channel, (along with the information for locating the broadcast channel), or frequently transmit SKI_B on the broadcast channel. The more often that the BS "refreshes" the value of SKI_B, the faster the MS 300 can access the broadcast message. The desire to refresh SKI_B data is balanced

against optimizing available bandwidth, as transmitting SKI_B data too frequently may use an unacceptable amount of bandwidth in the control channel or broadcast channel.

[1072] This paragraph discusses the encryption and transmission of the broadcast content. The CS encrypts the broadcast content using the current SK. The exemplary embodiment employs an encryption algorithm such as the Advanced Encryption Standard (AES) Cipher Algorithm. In the exemplary embodiment, the encrypted content is then transported by an IPsec packet according to the Encapsulating Security Payload (ESP) transport mode. The IPsec packet also contains an SPI value that instructs the ME 306 to use the current SK to decrypt received broadcast content. The encrypted content is sent via the broadcast channel.

[1073] Receive circuitry 304 provides the RKI and BAKI directly to the UIM 308. Further, receive circuitry 304 provides the SKI_B to an appropriate part of the MS 300 where it is combined with SKI_A to obtain SKI. The SKI is provided to the UIM 308 by the relevant part of the MS 300. The UIM 308 computes RK from the RKI and A-key, decrypts the BAKI using the RK to obtain BAK, and computes the SK using the SKI and BAK, to generate an SK for use by the ME 306. The ME 306 decrypts the broadcast content using the SK. The UIM 308 of the exemplary embodiment is not sufficiently powerful for decryption of broadcast content in real time, and, therefore, SK is passed to the ME 306 for decrypting the broadcast content.

[1074] FIG. 5 illustrates the transmission and processing of keys RK, BAK and SK according to the exemplary embodiment. As illustrated, at registration the MS 300 receives the RKI and passes it to UIM 308, wherein the SUPU 316 computes RK using RKI and the A-key, and stores the RK in UIM memory storage SUMU 314. The MS 300 periodically receives the BAKI that contains BAK encrypted using the RK value specific to UIM 308. The encrypted BAKI is decrypted by SUPU 316 to recover the BAK, which is stored in UIM memory storage SUMU 314. The MS 300 further periodically receives an SKI_B that it combines with SKI_A to form SKI. The SUPU 316 computes SK from SKI and BAK. The SK is provided to ME 306 for decrypting broadcast content.

[1075] In the exemplary embodiment the CS keys are not necessarily encrypted and transmitted to the MSs; the CS may use an alternative method.

The key information generated by the CS for transmission to each MS provides sufficient information for the MS to calculate the key. As illustrated in the system 350 of FIG. 6, the RK is generated by the CS, but RK information (RKI) is transmitted to the MS. The CS sends information sufficient for the UIM to derive the RK, wherein a predetermined function is used to derive the RK from transmitted information from the CS. The RKI contains sufficient information for the MS to determine the original RK from the A_key and other values, such as system time, using a predetermined public function labeled d1, wherein:

$$[1076] \quad RK = d1(A_key, RKI). \quad (3)$$

[1077] In the exemplary embodiment, the function d1 defines a cryptographic-type function. According to one embodiment, RK is determined as:

$$[1078] \quad RK = SHA'(A_key || RKI), \quad (4)$$

[1079] wherein "||" denotes the concatenation of the blocks containing A_key and RKI, and SHA'(X) denotes the last 128-bits of output of the Secure Hash Algorithm SHA-1 given the input X. In an alternative embodiment, RK is determined as:

$$[1080] \quad RK = AES(A_key, RKI), \quad (5)$$

[1081] wherein AES(X,Y) denotes the encryption of the 128-bit block RKI using the 128-bit A_key. In a further embodiment based on the AKA protocol, RK is determined as the output of the 3GPP key generation function f3, wherein RKI includes the value of RAND and appropriate values of AMF and SQN as defined by the standard.

[1082] The BAK is treated in a different manner because multiple users having different values of RK must compute the same value of BAK. The CS may use any technique to determine BAK. However, the value of BAKI associated with a particular UIM 308 must be the encryption of BAK under the unique RK associated with that UIM 308. The SUPU 316 decrypts BAKI using RK stored in the SUMU 314 according to the function labeled d2, according to:

$$[1083] \quad BAK = d2(BAKI, RK). \quad (9)$$

[1084] In an alternate embodiment, the CS may compute BAKI by applying a decryption process to BAK using RK, and the SUPU 316 obtains BAK by applying the encryption process to BAKI using RK. This is considered equivalent to the CS encrypting BAK and the SUPU 316 decrypting BAKI.

Alternate embodiments may implement any number of key combinations in addition to or in place of those illustrated in FIG. 6.

[1085] The SK is treated in a similar manner to RK. First SKI is derived from the SKI_A and SKI_B (SKI_B is the information transmitted from CS to MS). Then a predetermined function labeled d3 is used to derive the SK from SKI and BAK (stored in the SUMU 314), according to:

$$[1086] \quad SK = d3(BAK, SKI). \quad (6)$$

[1087] In one embodiment, the function d3 defines a cryptographic-type function. In an exemplary embodiment, SK is computed as:

$$[1088] \quad SK = SHA(BAK || SKI), \quad (7)$$

[1089] while in another embodiment, SK is computed as

$$[1090] \quad SK = AES(BAK, SKI). \quad (8)$$

[1091] A method of providing the security for a broadcast message is illustrated in FIGs. 7A-7D. FIG. 7A illustrates a registration process 400 wherein a subscriber negotiates registration with the CS at step 402. The registration at step 404 provides the UIM a unique RK. The UIM stores the RK in a Secure Memory Unit (SUMU) at step 406. FIG. 7B illustrates subscription processing 420 between a CS and a MS. At step 422 the CS generates a BAK for a BAK time period T1. The BAK is valid throughout the BAK time period T1, wherein the BAK is periodically updated. At step 424 the CS authorizes the UIM to have access to the Broadcast Content (BC) during the BAK timer period T1. At step 426 the CS encrypts the BAK using each individual RK for each subscriber. The encrypted BAK is referred to as the BAKI. The CS then transmits the BAKI to the UIM at step 428. The UIM receives the BAKI and performs decryption using the RK at step 430. The decrypted BAKI results in the originally generated BAK. The UIM stores the BAK in a SUMU at step 432. The UIM then receives the broadcast session and is able to access the BC by applying the BAK to decryption of the encrypted broadcast (EBC).

[1092] FIG. 7C illustrates a method of updating keys for security encryption in a wireless communication system supporting broadcast service. The method 440 implements time periods as given in FIG. 7E. The BAK is updated periodically having a time period T1. A timer t1 is initiated when BAK is calculated and times out at T1. A variable is used for calculating the SK referred to as SK_RAND, which is updated periodically having a time period T2.

A timer t2 is initiated when the SK RAND is generated and times out at T2. In one embodiment, the SK is further updated periodically having a period of T3. A timer t3 is initiated when each SK is generated and times out at time T3. The SK RAND is generated at the CS and provided periodically to the MS. The MS and the CS use SK RAND to generate the SK, as detailed hereinbelow.

[1093] A first timer t1 is reset when the applicable value of BAK is updated. The length of time between two BAK updates is the BAK update period. In the exemplary embodiment the BAK update period is a month, however, alternate embodiments may implement any time period desired for optimum operation of the system, or to satisfy a variety of system criteria.

[1094] Continuing with FIG. 7C, the method 440 initializes the timer t2 at step 442 to start the SK REG time period T2. The CS generates SK RAND and provides the value to transmit circuitry for transmission throughout the system at step 444. The timer t3 is initialized at step 446 to start the SK time period T3. The CS then encrypts the BC using the current SK at step 448. The encrypted product is the EBC, wherein the CS provides the EBC to transmit circuitry for transmission in the system. If the timer t2 has expired at decision diamond 450, processing returns to step 442. While t2 is less than T2, if the timer t3 has expired at decision diamond 452, processing returns to step 446; also processing returns to 450.

[1095] FIG. 7D illustrates the operation of the MS accessing a broadcast service. The method 460 first synchronizes the timers t2 and t3 with the values at the CS at step 462. The UIM of the MS receives the SK RAND generated by the CS at step 464. At step 466 the UIM generates the SK using the SK RAND, BAK, and a time measurement. The UIM passes the SK to the ME of the MS. The UIM then decrypts the received EBC using the SK to extract the original BC at step 468. When the timer t2 expires at step 470 processing returns to step 462. While the timer t2 is less than T2, if the timer t3 expires at step 472, the timer t3 is initialized at step 474 and returns to 466.

[1096] When the user subscribes to the broadcast service for a particular BAK update period, the CS sends the appropriate information BAKI (corresponding to the BAK encrypted with the RK). This typically occurs prior to the beginning of this BAK update period or when the MS first tunes to the broadcast channel during this BAK update period. This may be initiated by the

MS or CS according to a variety of criteria. Multiple BAKI may be transmitted and decrypted simultaneously.

[1097] Note that when expiration of the BAK update period is imminent, the MS may request the updated BAK from the CS if the MS has subscribed for the next BAK update period. In an alternate embodiment the first timer t_1 is used by the CS, where upon expiration of the timer, i.e., satisfaction of the BAK update period, the CS transmits the BAK.

[1098] Note that it is possible for a user to receive a BAK during a BAK update period, wherein, for example, a subscriber joins the service mid-month when the BAK updates are performed monthly. Additionally, the time periods for BAK and SK updates may be synchronized, such that all subscribers are updated at a given time.

[1099] FIG. 8A illustrates the registration process in a wireless communication system 500 according to the exemplary embodiment. The CS 502 negotiates with each subscriber, i.e., MS 512, to generate a specific RK to each of the subscribers. The RK is provided to the SUMU unit within the UIM of each MS. As illustrated, the CS 502 generates RK_1 which is stored in SUMU₁ 510 within UIM₁ 512. Similarly, the CS 502 generates RK_2 and RK_N which are stored in SUMU₂ 520 within UIM₂ 522 and SUMU_N 530 within UIM_N 532, respectively.

[1100] FIG. 8B illustrates the subscription process in the system 500. The CS 502 further includes multiple encoders 504. Each of the encoders 504 receives one of the unique RKs and the BAK value generated in the CS 502. The output of each encoder 504 is a BAKI encoded specifically for a subscriber. The BAKI is received at the UIM of each MS, such as UIM₁ 512. Each UIM includes a SUPU and a SUMU, such as SUPU₁ 514 and SUMU₁ 510 of UIM₁ 512. The SUPU includes a decoder, such as decoder 516 that recovers the BAK by application of the RK of the UIM. The process is repeated at each subscriber.

[1101] Key management and updates are illustrated in FIG. 8C, wherein the CS applies a function 508 to generate a value of SK_RAND, which is an interim value used by the CS and MS to calculate SK. Specifically, the function 508 applies the BAK value, the SK_RAND and a time factor. While the embodiment illustrated in FIG. 8C applies a timer to determine when to update the SK,

alternate embodiments may use alternate measures to provide periodic updates, for example occurrence of an error or other event. The CS provides the SK RAND value to each of the subscribers, wherein a function 518 resident in each UIM applies the same function as in function 508 of the CS. The function 518 operates on the SK RAND, BAK and a timer value to generate a SK that is stored in a memory location in the ME, such as MEM₁ 542 of ME₁ 540.

[1102] FIG. 8D illustrates the processing of BC after registration and subscription. The CS 502 includes an encoder 560 that encodes the BC using the current SK to generate the EBC. The EBC is then transmitted to the subscribers. Each MS includes an encoder, such as encoder 544, that extracts the BC from the EBC using the SK.

[1103] While the present invention has been described with respect to an exemplary embodiment of a wireless communication system supporting a unidirectional broadcast service, the encryption methods and key management described hereinabove is further applicable to other data processing systems, including a multi-cast type broadcast system. Still further, application of the present invention to any data processing system wherein multiple subscribers access a single transmission of secure information through an insecure channel.

[1104] Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[1105] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as

hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[1106] The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[1107] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

[1108] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to

WO 02/030449

PCT/US02/09835

27

other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

[1109] WHAT IS CLAIMED IS:

CLAIMS

1. A method for secure transmissions, the method comprising:
2 determining a registration key specific to a participant in a transmission;
4 encrypting the first key with the registration key;
6 determining a second key;
encrypting the second key with the first key; and
updating the first and second keys.
2 The method as in claim 1, wherein updating further comprises:
2 updating the first key according to a first time period; and
4 updating the second key according to a second time period, wherein the
second time period is less than the first time period.
3. The method as in claim 2, wherein updating further comprises:
2 encrypting an updated first key with the registration key ; and
encrypting an updated second key with the updated first key.
4 The method as in claim 2, further comprising:
2 encrypting a broadcast stream of information using the second key; and
transmitting the encrypted broadcast stream of information.
5. The method as in claim 4, wherein the broadcast stream of information
2 comprises video information.
6. The method as in claim 4, wherein the broadcast stream of information
2 comprises Internet Protocol packets.
7. The method as in claim 3, further comprising:
2 calculating a registration key information message; and
transmitting the registration key information message.

WO 02/050449

PCT/US02/09335

29

8. The method as in claim 7, further comprising:
2 calculating a first key information message corresponding to the updated
and encrypted first key; and
4 transmitting the first key information message.
9. The method as in claim 8, further comprising:
2 calculating a second key information message corresponding to the
updated and encrypted second key; and
4 transmitting the second key information message.
10. The method as in claim 1, further comprising:
2 transmitting the encrypted first key; and
transmitting the encrypted second key.
11. A method for secure reception of a transmission, the method comprising:
2 receiving a registration key specific to a participant in a transmission;
receiving a first key;
4 decrypting the first key with the registration key;
receiving a second key;
6 decrypting the second key with the first key;
receiving a broadcast stream of information; and
8 decrypting the broadcast stream of information using the second key.
12. The method as in claim 11, further comprising:
2 storing the first key in a secure memory storage unit; and
storing the second key in a memory storage unit.
13. The method as in claim 11, further comprising:
2 recovering the first key from a first key information message; and
recovering the second key from a second key information message.
14. The method as in claim 11, further comprising:
2 updating the first key according to a first time period; and
updating the second key according to a second time period.

15. In a wireless communication system supporting a broadcast service option,
2 an infrastructure element comprising:
a receive circuitry;
4 a user identification unit, operative to recover a short-time key for
decrypting a broadcast message, comprising:
6 processing unit operative to decrypt key information;
memory storage unit for storing a registration key; and
8 a mobile equipment unit adapted to apply the short-time key for
decrypting the broadcast message.
16. The infrastructure element as in claim 15, wherein the short-time key is
2 processed by the user identification unit and passed to the mobile equipment
unit.
17. The infrastructure element as in claim 15, wherein the memory storage unit
2 is a secure memory storage unit.
18. The infrastructure element as in claim 15, wherein the memory storage unit
2 stores a broadcast access key, and wherein the processing unit decrypts the
short-time key using the broadcast access key.
19. The infrastructure element as in claim 18, wherein the short-time key is
2 updated at a first frequency.
20. The infrastructure element as in claim 19, wherein the broadcast access key
2 is updated at a second frequency less than the first frequency.
21. The infrastructure element as in claim 15, wherein the broadcast service
2 option is a video service.
22. A wireless communication system, comprising:
2 means for determining a registration key specific to a participant in a
transmission;

WO 02/060449

PCT/US02/09835

31

- 4 means for determining a first key;
means for encrypting the first key with the registration key;
- 6 means for determining a second key;
means for encrypting the second key with the first key; and
- 8 means for updating the first and second keys.

23. An infrastructure element, comprising:

- 2 means for receiving a registration key specific to a participant in a
transmission;
- 4 means for receiving a first key;
means for decrypting the first key with the registration key;
- 6 means for receiving a second key;
means for decrypting the second key with the first key;
- 8 means for receiving a broadcast stream of information; and
means for decrypting the broadcast stream of information using the
- 10 second key.

24. A digital signal storage device, comprising:

- 2 first set of instructions for receiving a registration key specific to a
participant in a transmission;
- 4 second set of instructions for receiving a first key;
third set of instructions for decrypting the first key with the registration
- 6 key;
- fourth set of instructions for receiving a second key;
- 8 fifth set of instructions for decrypting the second key with the first key;
sixth set of instructions for receiving a broadcast stream of information;
- 10 and
- seventh set of instructions for decrypting the broadcast stream of
- 12 information using the second key.

WO 02/050449

PCT/ES02/09935

1/15

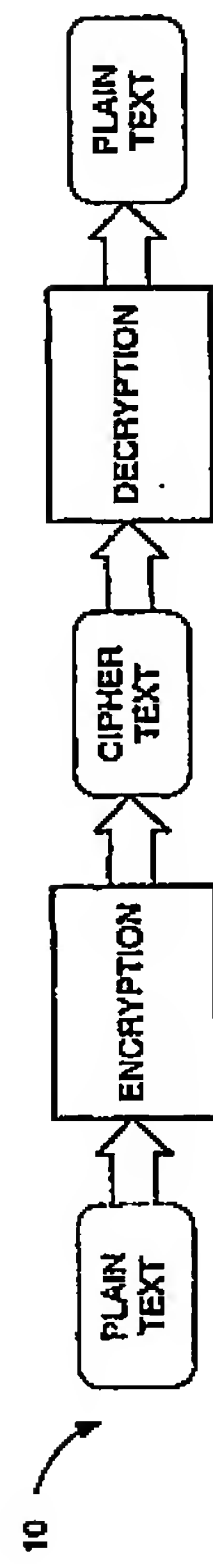


FIG. 1A

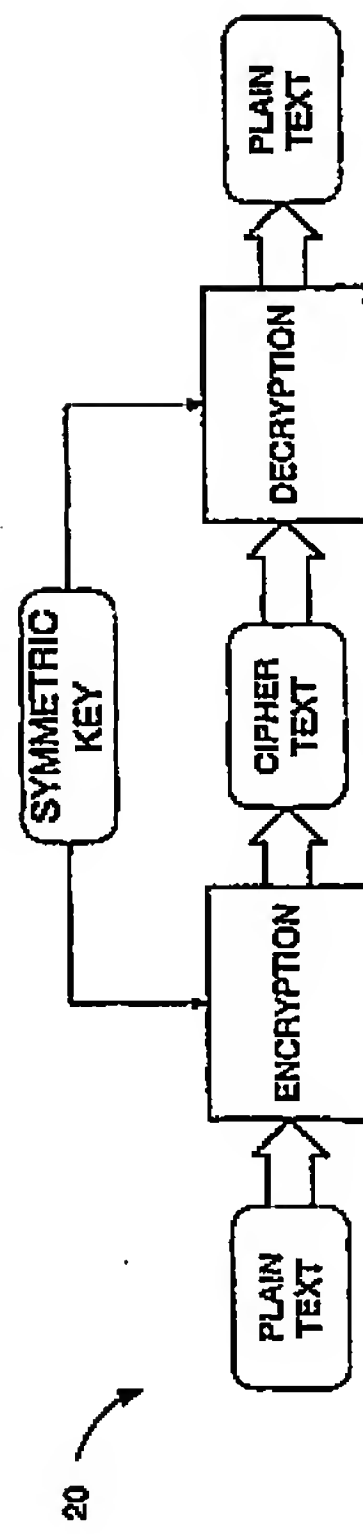


FIG. 1B

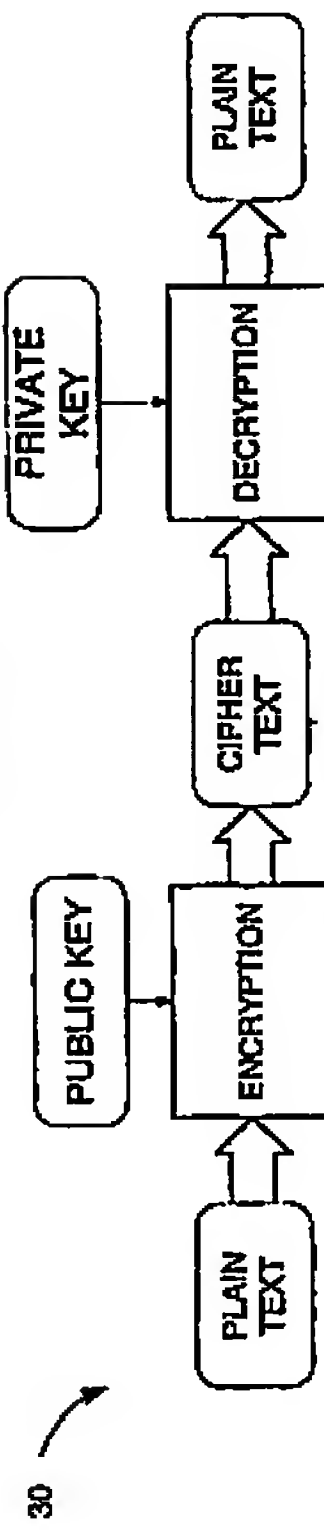
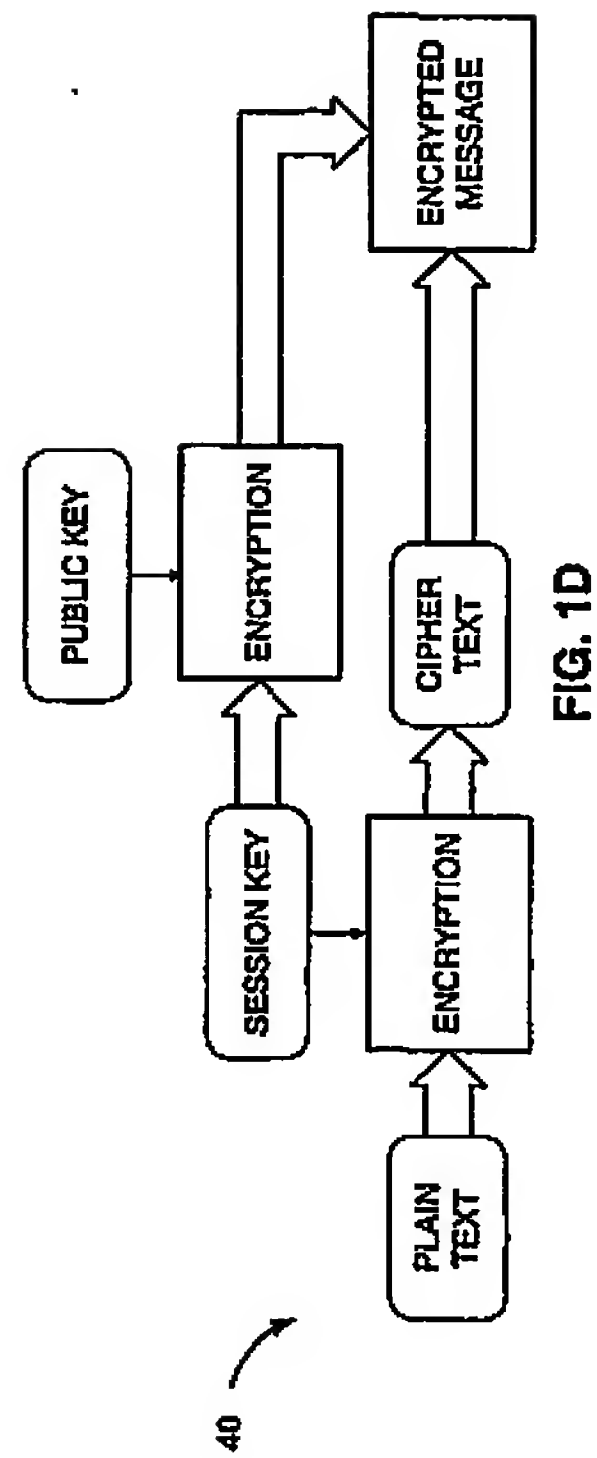


FIG. 1C

WO 02/050449

PCT/US02/09835

2/15



WD 02/030449

PCT/US02/09835

3/15

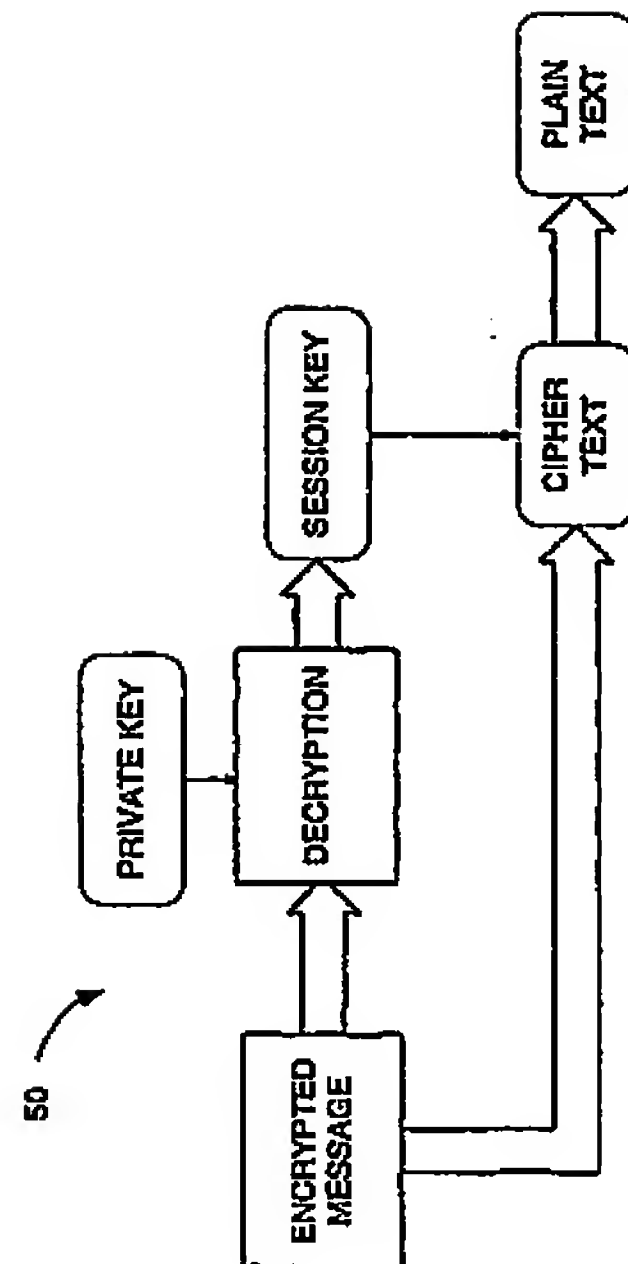
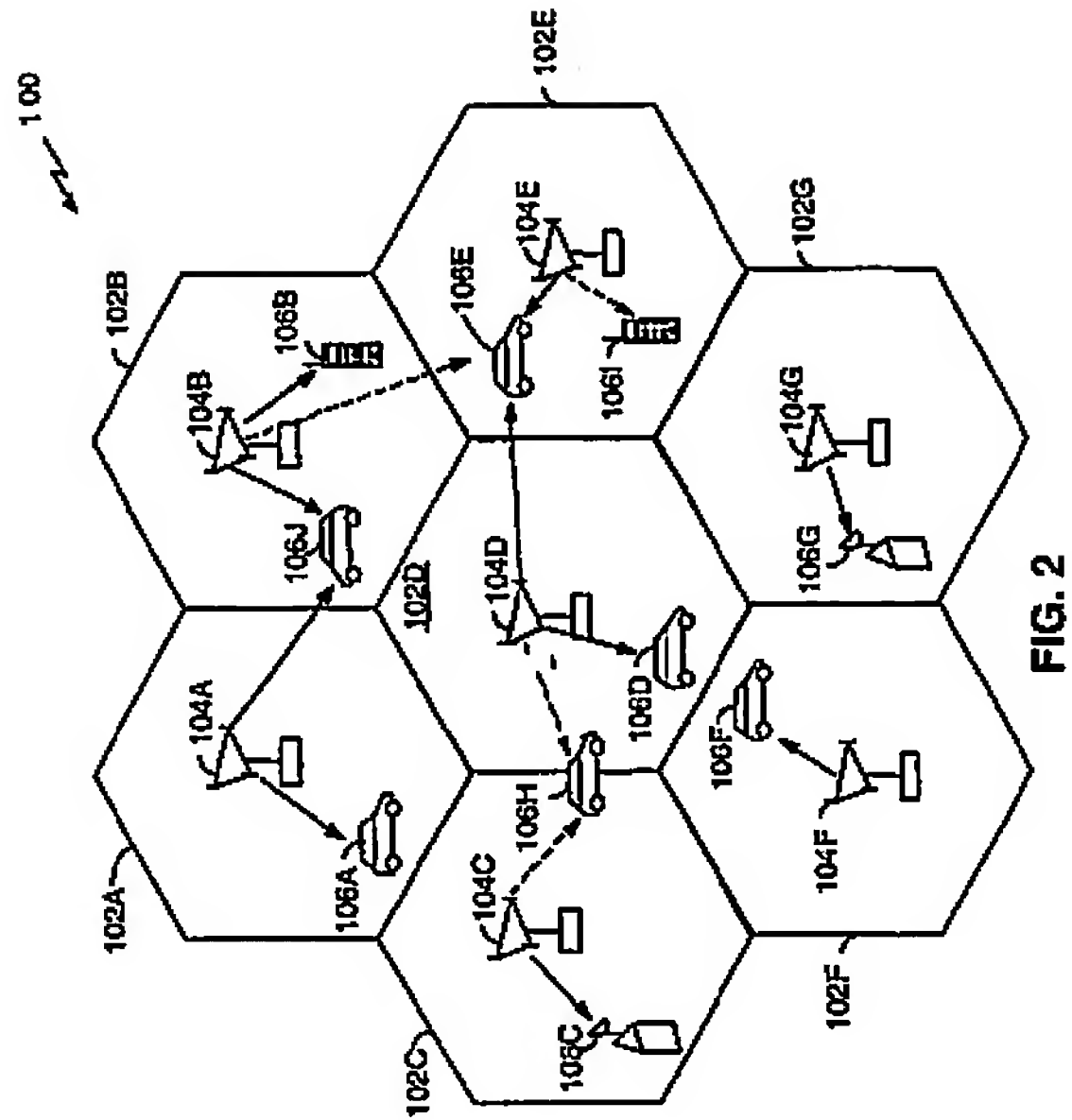


FIG. 1E



WO 02/030449

PCT/US02/09835

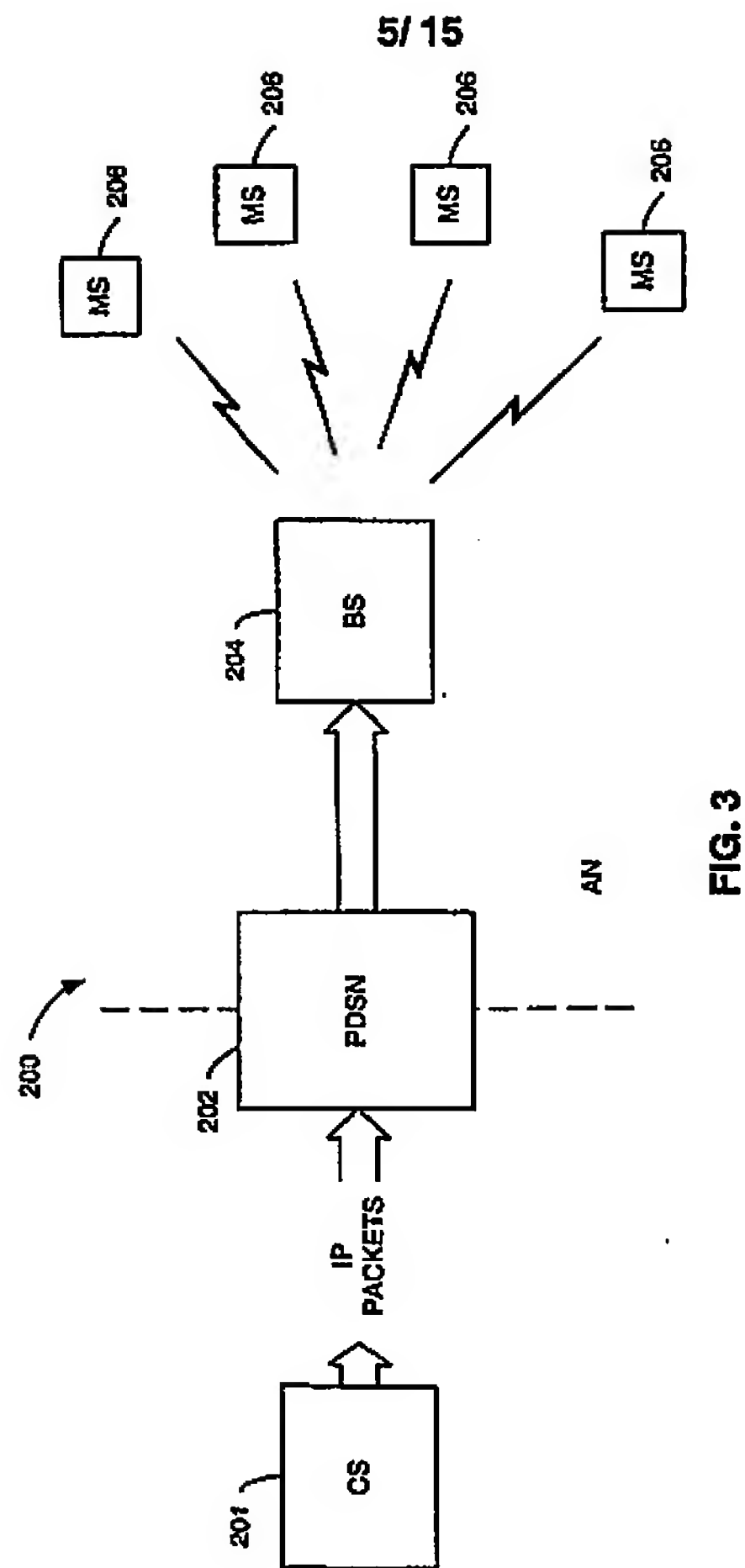


FIG. 3

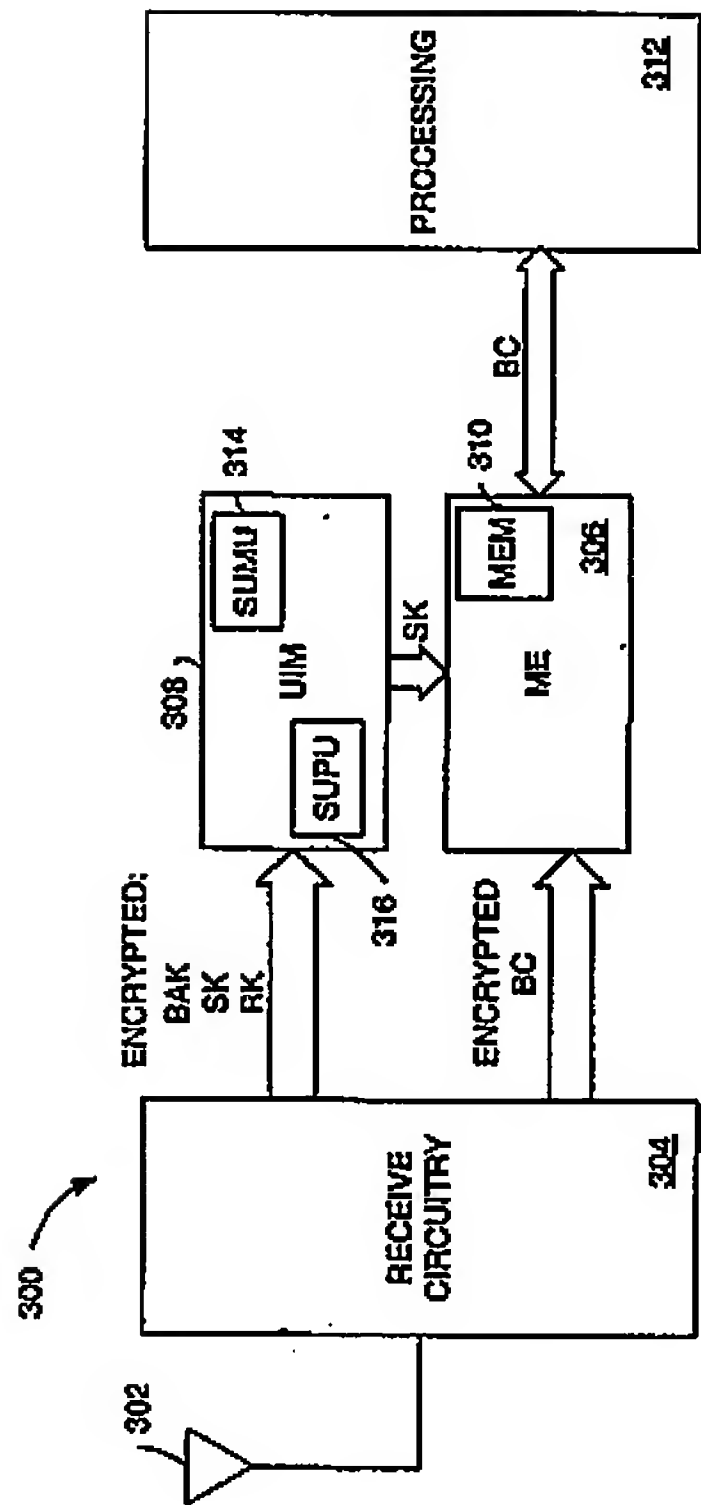
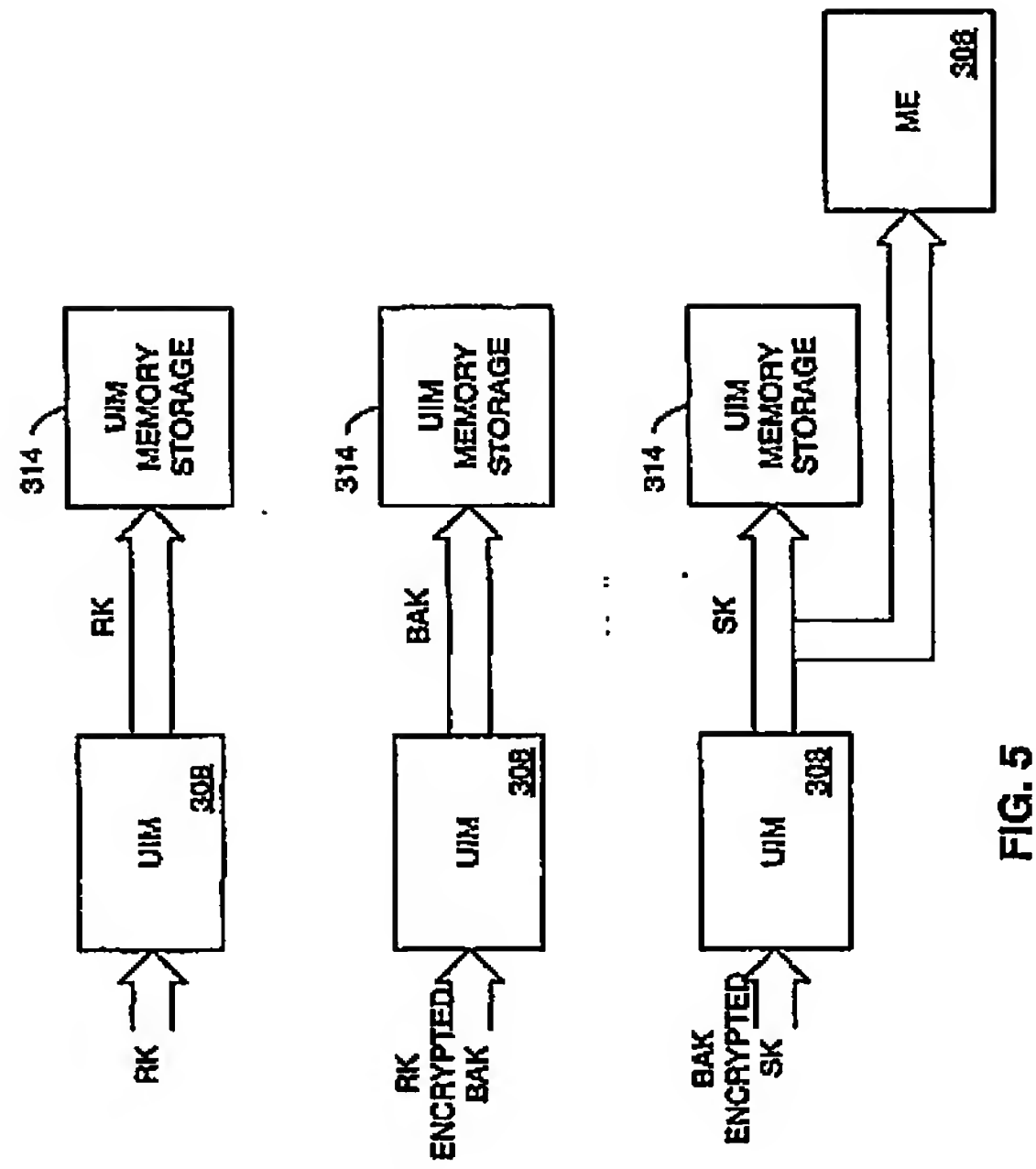


FIG. 4

WO 02/030449

PCT/US02/09335

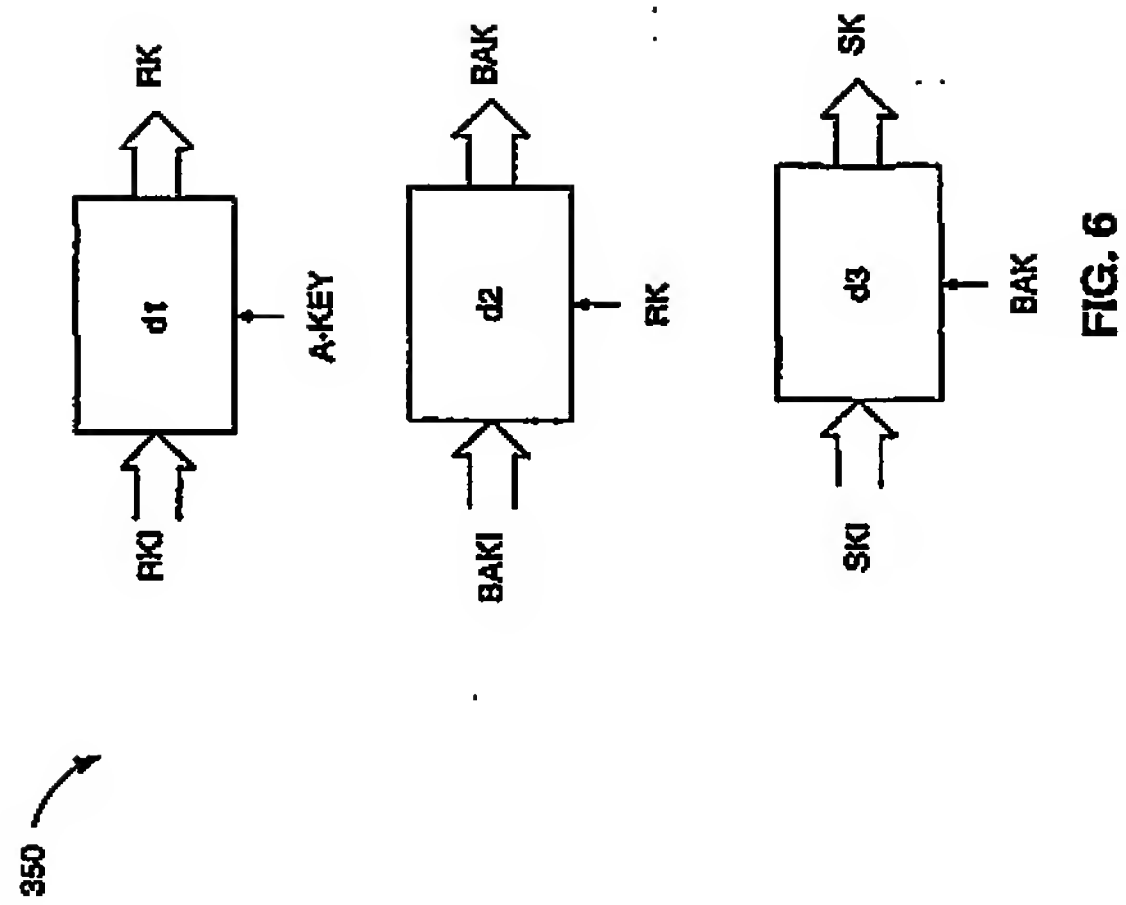
7/15



WO 02/060449

PCT/US02/09235

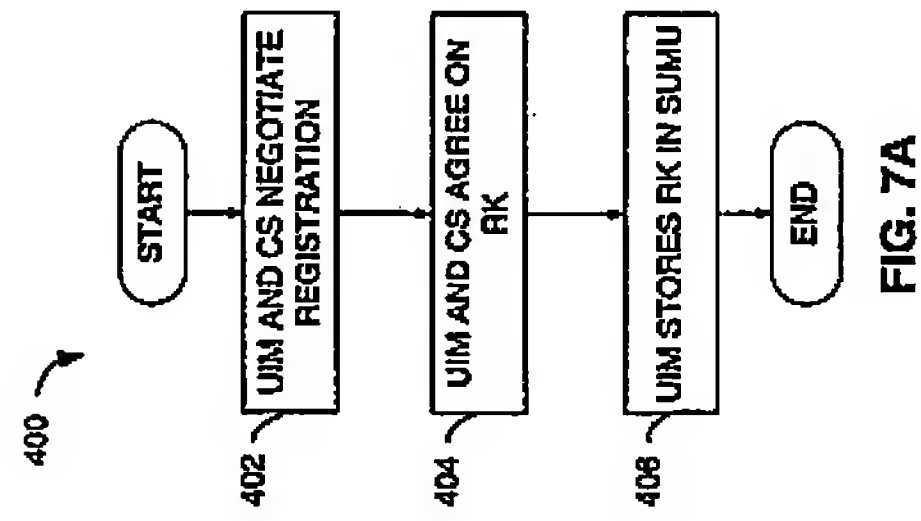
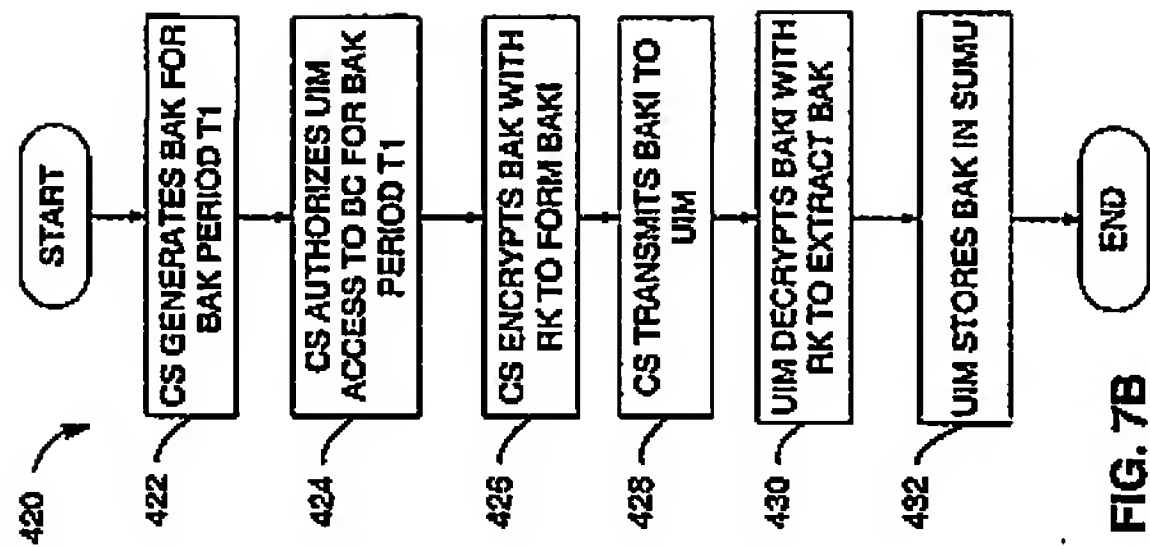
8/15



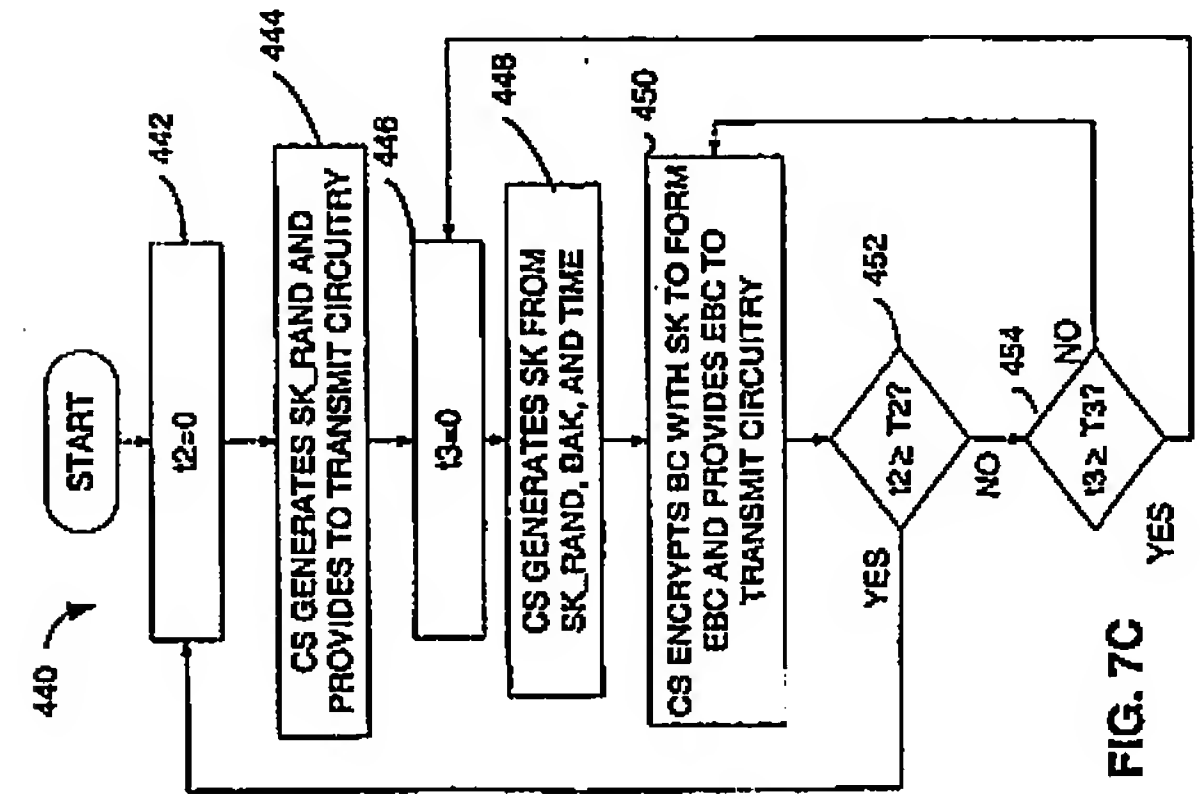
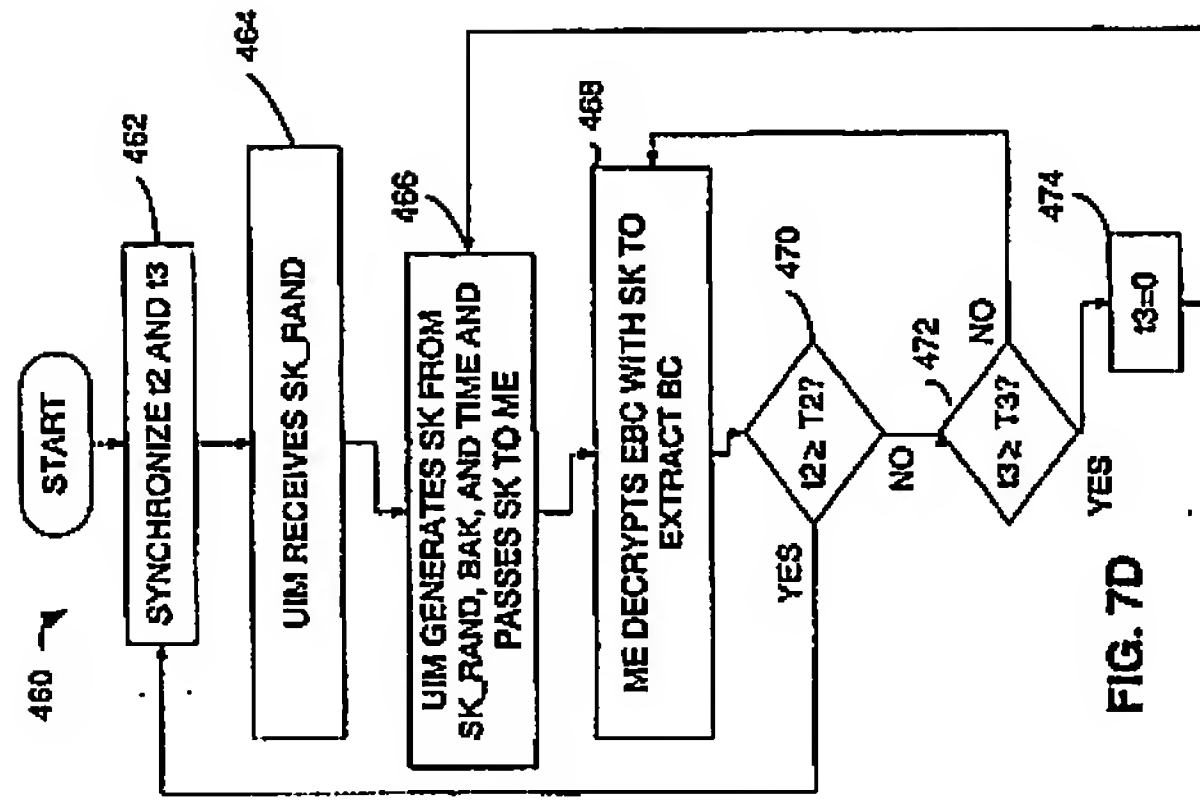
WO 02/050449

PCT/US02/09835

9/15



10/15



WD 02/050449

PCT/US02/09835

11/15

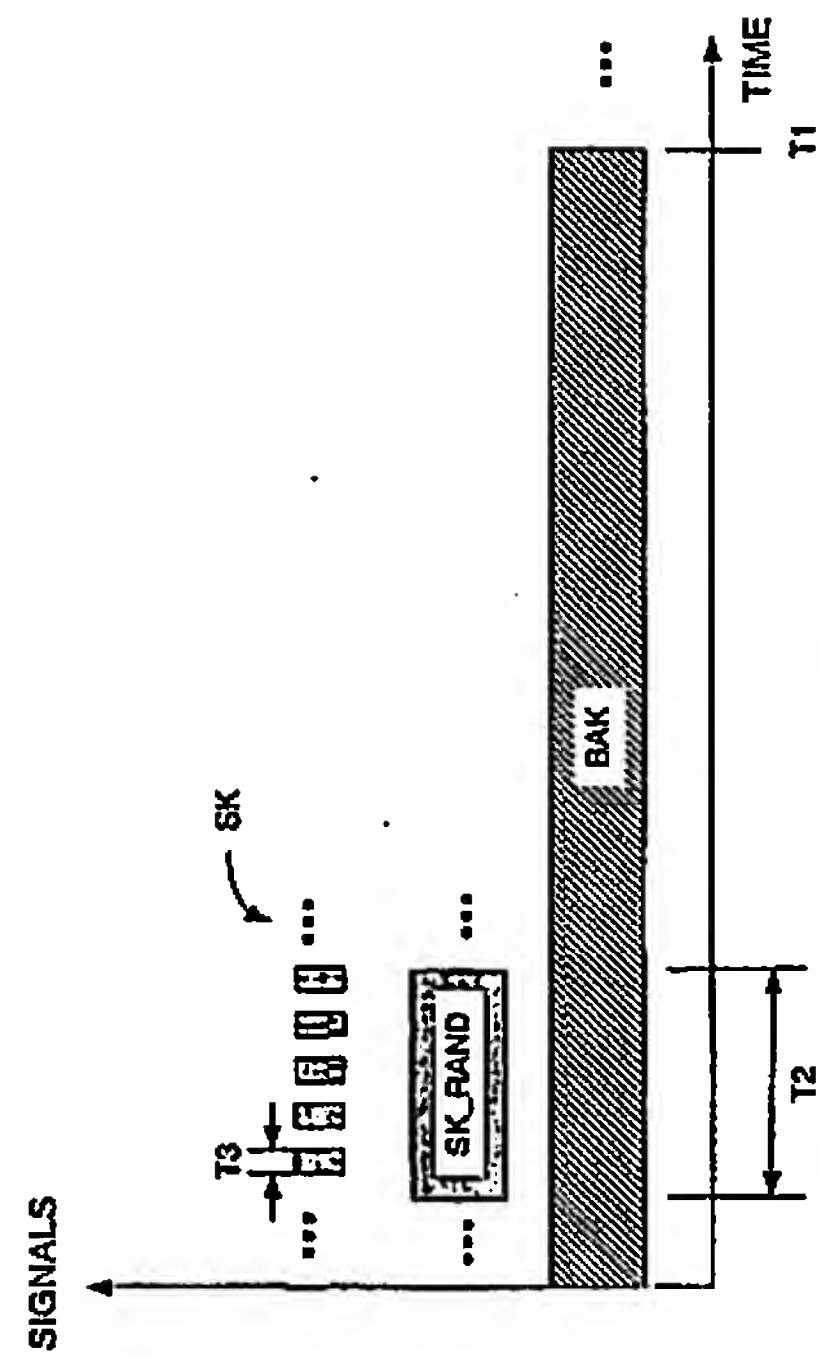


FIG. 7E

WD 02/030449

PCT/US02/09335

12/15

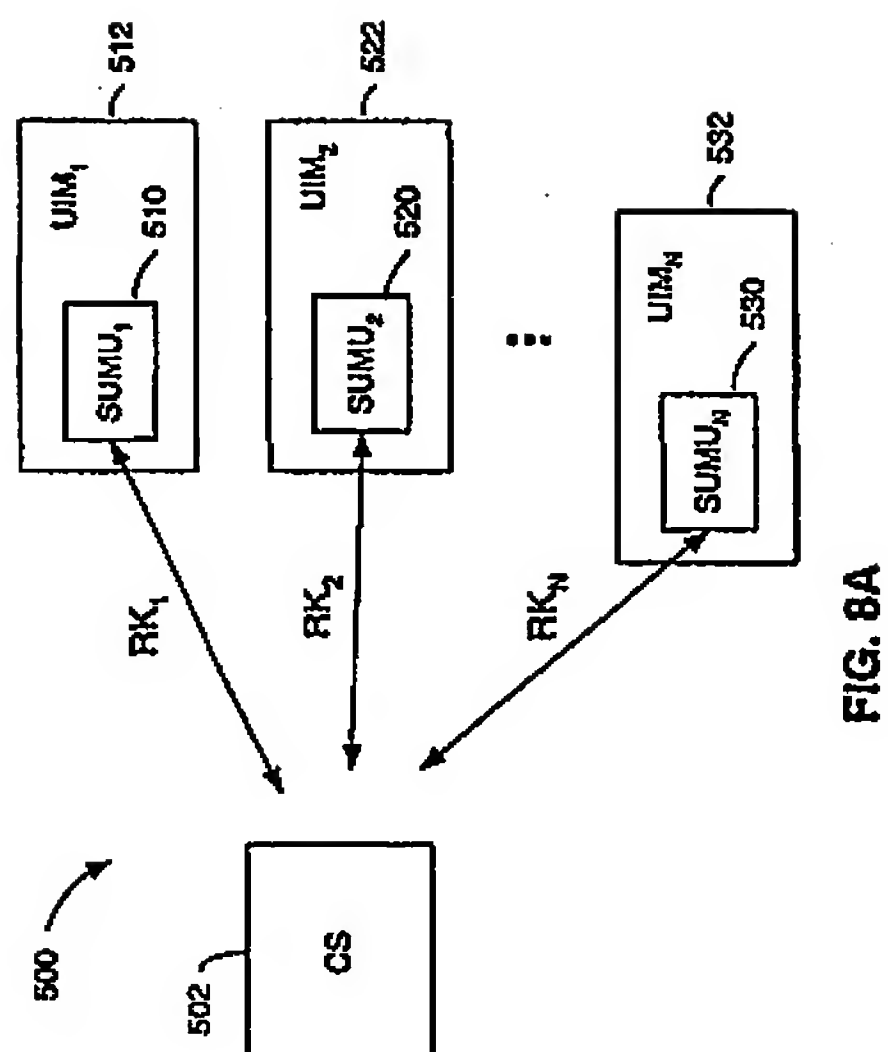


FIG. 8A

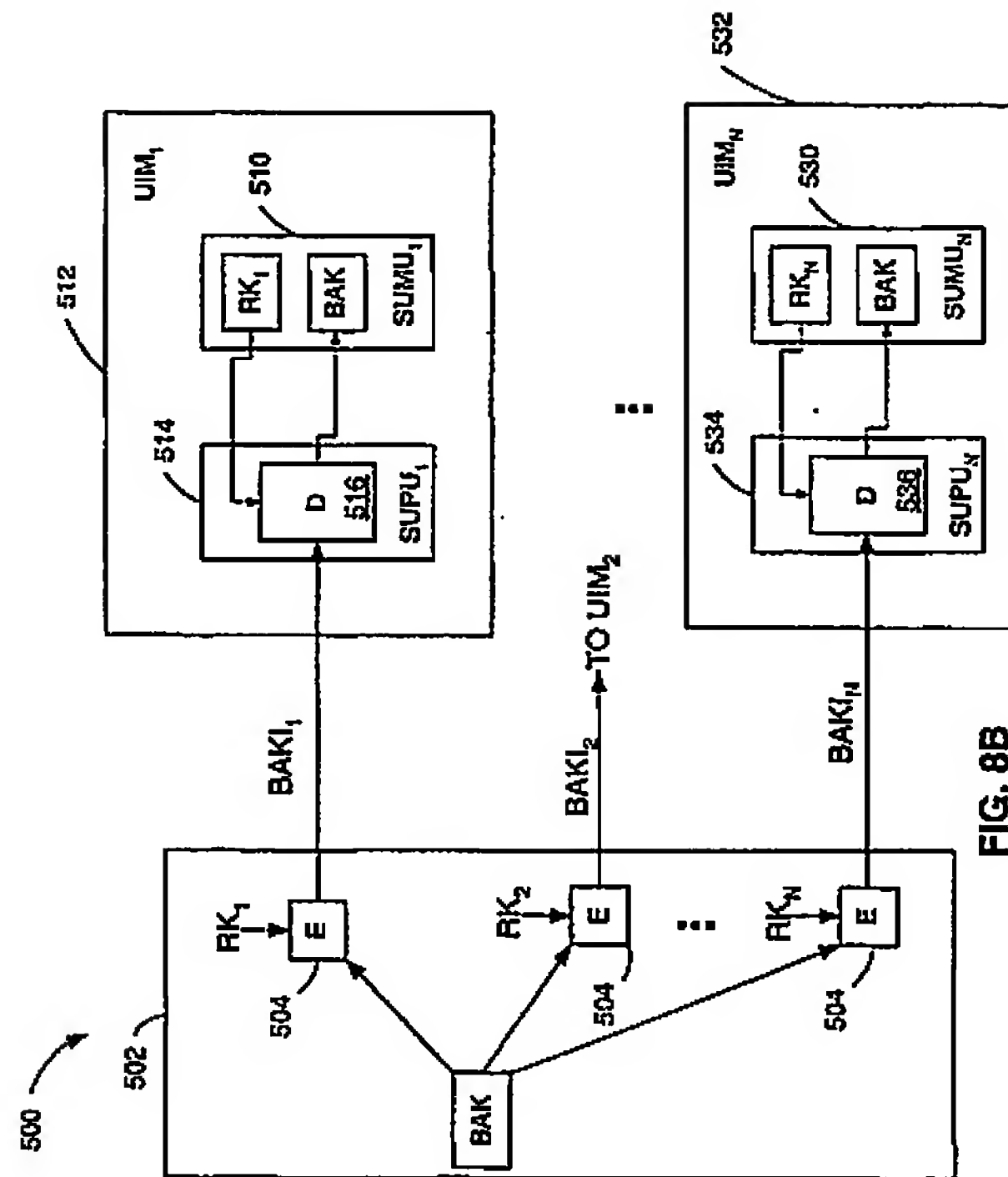


FIG. 8B

WO 02/030449

PCT/US02/09315

14/ 15

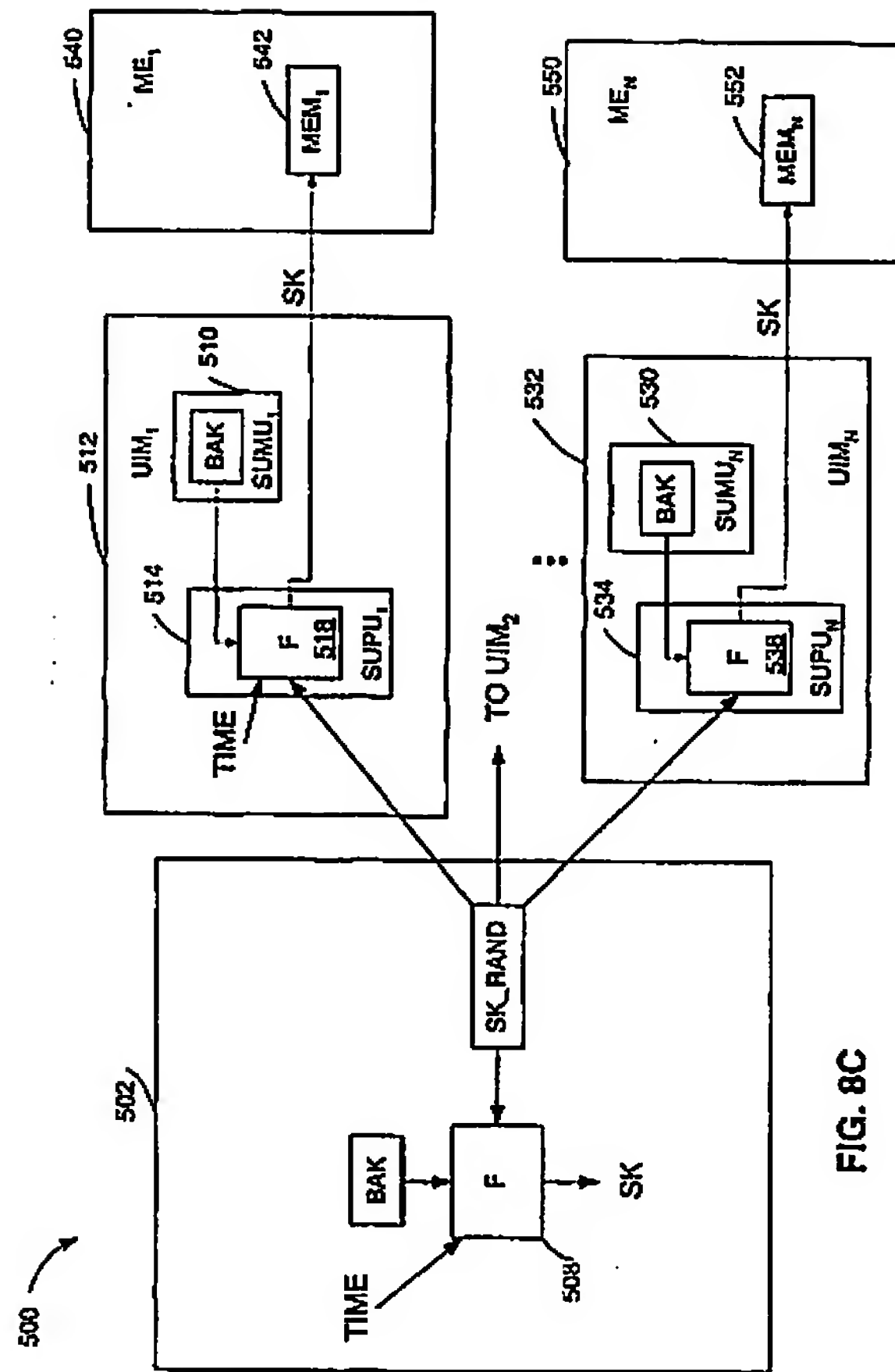


FIG. 8C

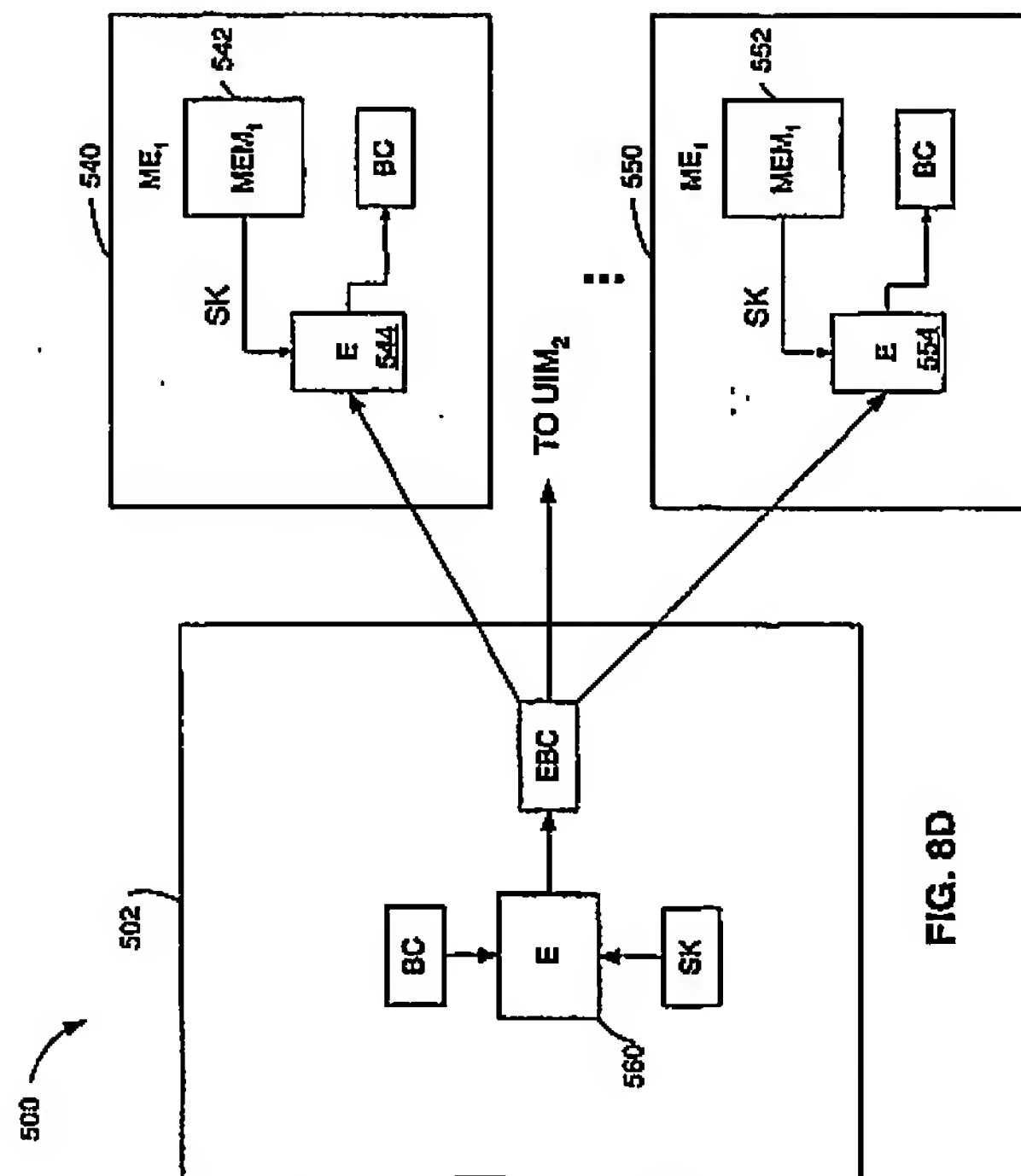


FIG. 8D

Page 1 of 2

INTERNATIONAL SEARCH REPORT		FCI/US 02/09835
C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim no.
A	<p>MARCHENT B G ET AL: "Intelligent control of mobile multimedia systems" VEHICULAR TECHNOLOGY CONFERENCE, 1998. VTC 98. 48TH IEEE OTTAWA, ONT., CANADA 18-21 MAY 1998, NEW YORK, NY, USA, IEEE, US, 18 May 1998 (1998-05-18), pages 2047-2051, XP010288261 ISBN: 0-7803-4320-4 the whole document</p>	5,6,21

From PCT/AA270 (publication of second sheet) (July 1997)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT, BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN, TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE, GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,P L,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZM,ZW

(74)代理人 100084618

弁理士 村松 貞男

(74)代理人 100092196

弁理士 橋本 良郎

(72)発明者 ホークス、フィリップ

オーストラリア国、ニューサウスウェールズ州 2134、バーウッド、ベルモア・ストリート、
ユニット2/6-8

(72)発明者 ローズ、グレゴリー・ジー

オーストラリア国、ニューサウスウェールズ州 2137、モルトレイク、キングストン・アベニ
ュー 6

(72)発明者 シュー、レイモンド・ティー

アメリカ合衆国、カリフォルニア州 92127、サン・ディエゴ、ペンナクック・コート 17
775

(72)発明者 レザイーファー、ラミン

アメリカ合衆国、カリフォルニア州 92131、サン・ディエゴ、カミニト・アルカダ 108
96

Fターム(参考) 5J104 AA01 AA12 AA16 AA34 BA03 EA01 EA04 EA15 EA18 JA03

MA05 NA02 NA37 PA01 PA05

5K067 AA32 BB03 BB04 CC04 CC10 EE23 HH36